

# Common mode and coupled failure

**Taylor, J.R.**

*Publication date:*
1976

*Document Version*
Publisher's PDF, also known as Version of record

A. E. K. Risø

Risø - M - 1826

Risø - M - 1826

Title and author(s)

Common Mode and Coupled Failure

by

J.R. Taylor

Date October 1975

Department or group

Electronics

Group's own registration number(s)

R-6-75

pages + tables + illustrations

Abstract

Based on examples and data from Abnormal Occurrence Reports for nuclear reactors, a classification of common mode or coupled failures is given, and some simple statistical models are investigated.

Copies to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, DK-4000 Roskilde, Denmark
Telephone: (03) 35 51 01, ext. 334, telex: 43116

F. 25-204

ISBN 87-550-0361-3

## CONTENTS

## 1. COMMON MODE AND COUPLED FAILURES, AN INTRODUCTION

### Introduction

In a series of studies of failures and abnormal occurrences in power plants, it has proved possible to gather some statistical information on common mode failure, and also to learn something of common mode failure phenomena.

In this note, the observations are brought together, and some of the theoretical problems are discussed. Some new data are presented.

"Common mode failure" has been defined in several different ways. One of the first studies (Epler 1969) was concerned with failures in similar redundant units:

> The failure of all members of a group in a single environment is a recognized possibility in industry where officers of a corporation are discouraged from riding as a group in a single aeroplane. Similarly, attorneys often advise their clients to provide in their wills for the possibility of both husband and wife being killed in a single accident; this, in legal circles, is known as the "common disaster". It would be expected that, when any group is made up of identical elements, all in the group would respond similarly to an externally applied stimulus; and, if failure resulted, this would be a common mode failure. When identical elements are used in a protection system, they are subject to simultaneous failure as a result of a single event.

In the "Rasmussen report" (WASH-1400 Draft, Appendix IV 1974) a wider definition is given:

> With regard to the analyses performed in this study, common mode failures can be defined as multiple failures which are dependent, thereby causing independent probabilities to be in reality dependent probabilities. The multiple failures are common mode or dependent because they result from a single initiating cause.
> The single initiating cause can be any one of a number of possibilities: a common property, a common process, a common environment, or a common external event. The multiple failures

which are dependent and common mode can likewise encompass a spectrum of possibilities; multiple system failure caused by a common component failure, system failures caused by a common external event, multiple component failures caused by a common defective manufacturing process, a sequence of failures caused by a common human operator, etc.

Gangloff (1974), in describing a method for anticipating potential common mode failure problems, defines common mode failures as "multiple unit failures due to a single cause".

It is not easy to define common mode failure in a way which is sufficiently precise to allow consistent statistics to be collected. Some of the problems involved are discussed later and a definition offered.

The term "common mode failure" has tended to become "loaded", as being the most likely cause of "complete system failure" for many redundant systems. If one adopts one of the above definitions, and then attempts to collect statistical data concerning common mode failure, one finds, for nuclear power plant at least, that the incidence of "multiple unit failures due to a common cause" is relatively high. For these reasons, the term "coupled failure" is used to refer to such multiple failures, and the term "common mode failure" is reserved for those cases in which "coupled failures" cause a complete subsystem to fail in a non fail-safe mode.

The sections of this note deal with definition of coupled failure, classification, some theoretical considerations, a summary of statistical data collected in earlier studies, and some conclusions.

Classification of coupled failures is treated in detail in this note, before definition of the term "coupled failure" is attempted. It is hoped that in this way, motivation for some of the finer points in the definition can be explained.

## 2. CLASSIFICATION OF COUPLED FAILURES

Gangloff classified common mode failures according to cause (1974). The purpose of the classification was to provide a check list in discovering potential coupled failures.

"Common Mode Failure

Common mode failures are multiple unit failures due to a single cause. They are generally categorized by their cause into the five broad groups. Through such categories, the reliability engineer can focus on possibilities for common mode failure links in a systematic way and consider the potential causes one at a time. Five categories generally used with perhaps some variation are:

1) External normal environment: This group takes into account such common-mode causative factors as dust, dirt, humidity, and temperature which are the normal extremes of the operating environment.

2) Equipment design deficiency: This group takes account of design and installation features and practices which give rise to either electrical or mechanical interdependence between system components between subsystems of the same system, or upon a single common element. Also included in this group are those cases of dependence on equipment or parameters whose failure or abnormality causes the transient requiring protection.

3) Operation and maintenance errors: This group included carelessness, improper adjustment or calibration, improper maintenance, and other human factors which are inadvertant, but must be considered possible.

4) External phenomena: This included such natural events as tornado, fire, flood, and earthquake which can effect every system in the plant.

5) Functional deficiency: This group of factors covers those possibilities where the design may be inadequate either because of erroneous predictions about the behaviour or usefulness of variables monitored predictions of the effectiveness of protection action to be taken." (Gangloff 1974).

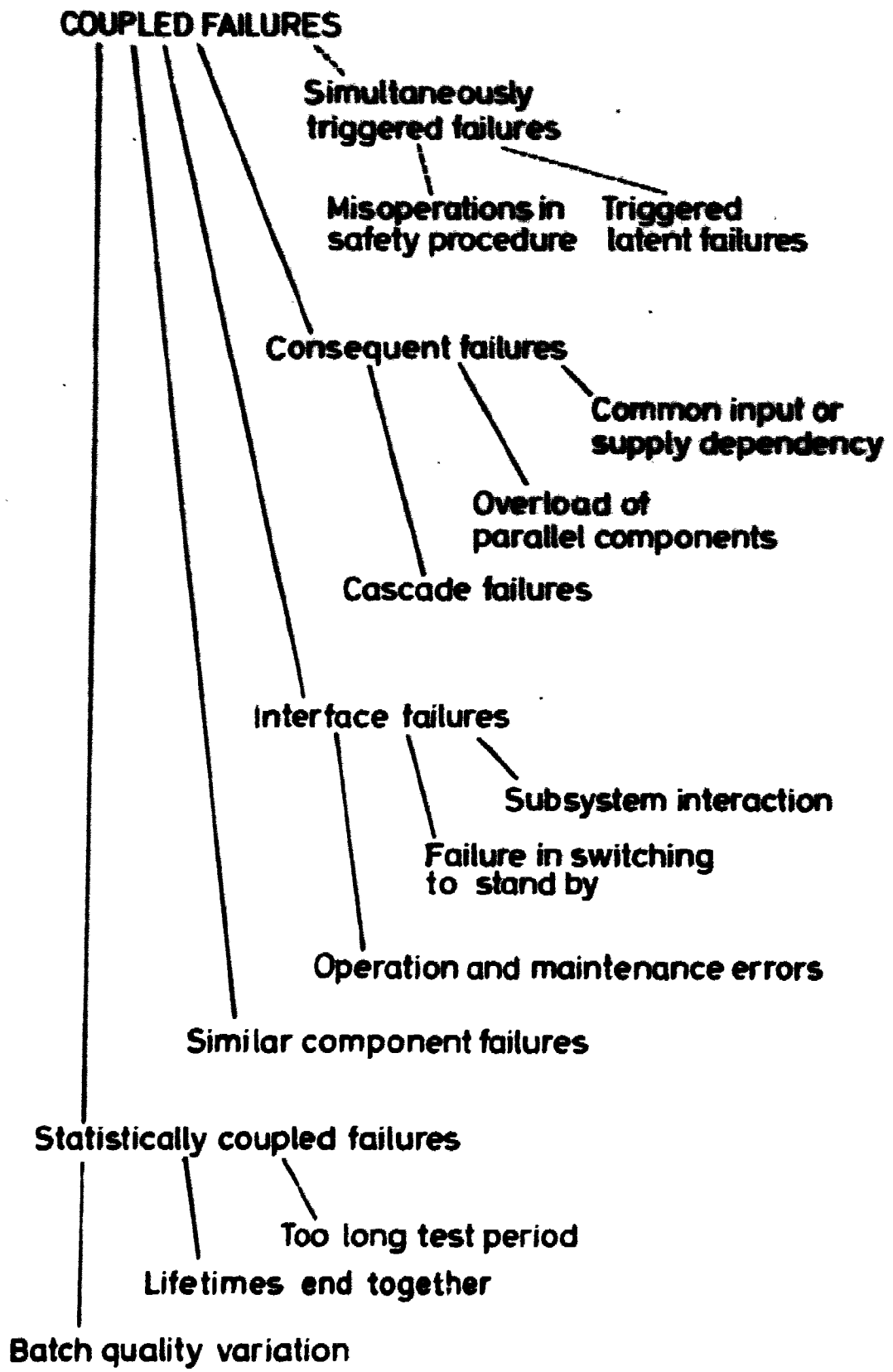



Fig. 1. Types of failure coupling.

The classification offered in this note is according to failure mechanism or process. The purpose is to provide a basis for a study of common mode failure probabilities. Failure types which grouped together in this classification, will require similar statistical models to predict their probability.

In Fig. 1 a classification is shown which covers all the types of coupled failures observed in the earlier studies. Some of the types of "coupling" are not the kind which one normally associates with common mode failure. These are shown with broken lines in the classification of Fig. 1 and are included for completeness. Most of the terms used require further clarification.

Triggered failures are those failures which can only make themselves felt as a result of some previous failure or unusual occurrence. There are two subclasses: misoperation failures in safety or shut down procedures; and triggered (revealed) latent failures. Triggered failures are not usually regarded as common mode failures. Triggered failures are included in this classification for completeness, but are not discussed further.

Consequent failures are those which are the direct result of some earlier failure. That is, some initial failure is the direct cause of the consequent failure. There are three subclasses; common dependency failures; parallel component overload failures; and cascade failures.

Common dependency failures are those in which two or more components fail because of the failure of some third component on which they are dependent. Failure of common power supplies, failure of common cooling air supplies, or failure of common supporting frameworks, give rise to examples.

Two mechanisms have been observed which give rise to overload coupled failures. In the first, some external event occurs which imposes on overload on two components operating in parallel. In the second, one component of a parallel pair fails, and in so doing puts an extra load or transient on its pair.

Cascade failures are those which arise when one component fails, and then destroys further components. Fire, flooding, excessive vibration, and missiles generated in an initial failure, can all give rise to cascade failures.

Interface failures are those which can occur when two systems are connected together. There are three subclasses, subsystem interactions, human operations common to both systems, and failures in switching between redundant subsystems.

The importance of distinguishing interface coupled failures is that, to take account of their effects, one can (hopefully) regard them as a perturbation or modification of the primary reliability analyses for subsystems (c.f. WASH 1400), without needing to treat an entire plant in each subsystem reliability analysis.

Similar component coupled failures are those which arise in components of the same type. These are the most common in practice, and the only class for which any statistical analysis has been attempted in this report.

For components which work intermittently or are subject to intermittent loads, varying requirements or environments, a clear distinction must made between the "cause" of a failure and its "trigger". The cause is the process or event which causes the component to be in a failed state, that is, unable to perform according to specifications in all specified circumstances. The failure may remain latent until some trigger event occurs. The trigger event is a normally occurring event, or at least, an event which would not normally lead to failure. If the component were not in a failed state, the component would perform correctly. But since failure has occurred, the trigger causes the latent failure to be revealed. A "failure to operate" occurs. For intermittently operating components "failures to operate" are of primary interest.

The types of coupling which have been observed in similar components in practice are

(a) Coupling due to failure rate variation of components from batch to batch, when two components are drawn from the same batch, or due to failure rate variation from installation to installation.

(b) Coupling due to joint variation of failure rates with time, for example due to wearout, infant mortality, or environment effects.

(c) Coupling due to variations in sensitivity to particular failure trigger events, from batch to batch of components or from

installation to installation.

(d) Coupling due to a common failure cause, which works immediately, or due to destructive effects of failure of one component on another. This group is similar to the "consequent failures" described earlier, but here is restricted to coupled failures in similar components.

These types of coupling provide a rational basis for classification according to cause, but unfortunately groups (a) and (b) are often difficult to distinguish from each other. Also there are large differences in the types of failures which can occur, depending on whether the components work intermittently, or continuously.

For these reasons, the following four groups were used in classifying data, according to the types of reliability models required in determining coupled mode failure probability:

I Failures due to design, installation errors etc. which cannot be detected during normal testing procedures, but which reveal themselves under unusual operating conditions. If the unusual conditions occur, then failure is generally certain. This grouping corresponds to coupling type (c) above. In the examples observed, the components were generally intermittently operated.

II Failures resulting from effects (poor design, installation, bad batch of components or environmental effects) leading to an unusually high failure rate during stand-by or ready waiting. There is then a higher than expected probability that several components will fail between activations or tests.

This grouping corresponds to classes (a) and (b) above. It was the most common type of coupled failure in the examples studied.

For this kind of failure, the frequency of coupled failure will vary, depending on test frequency. In practice, the distinction between continuously operating and intermittent, instantaneously operating triggers, is not so clear cut. For example the problem of environmental sensitivity of components, leading to latent failure, may be important over a period of a few days during the winter.

Some of these considerations are illustrated in figure 2.

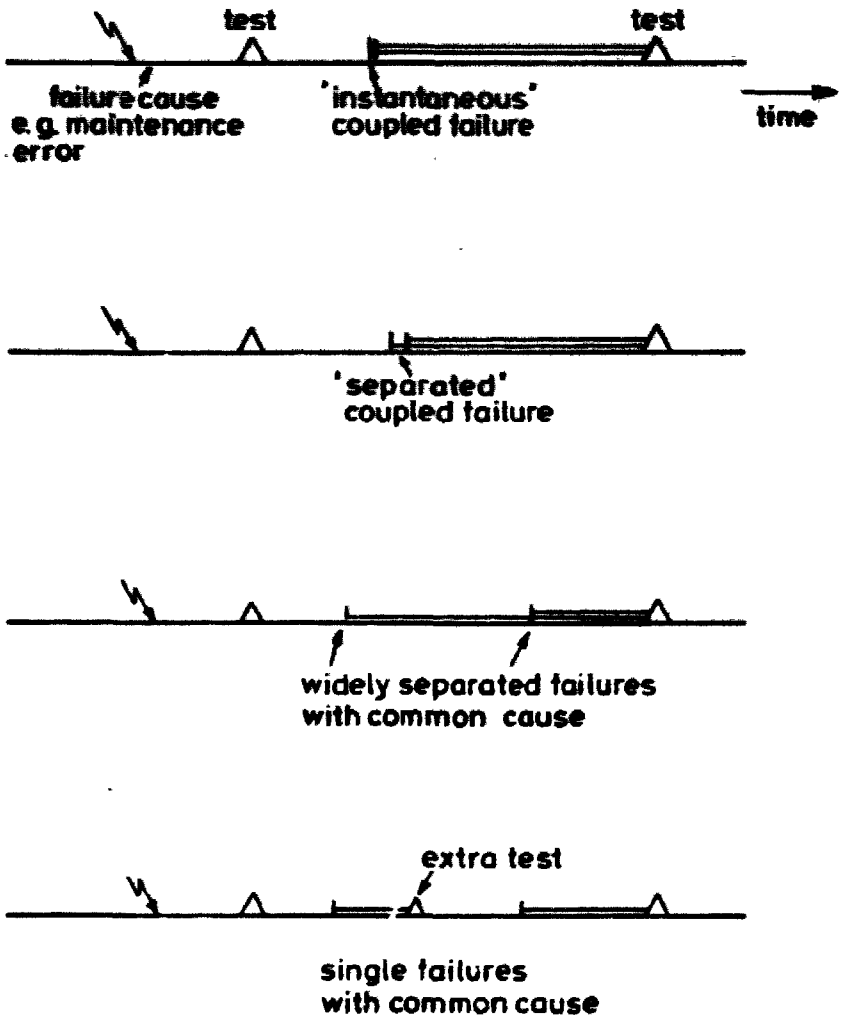



Fig. 2. Test interval dependence of coupled failure frequency

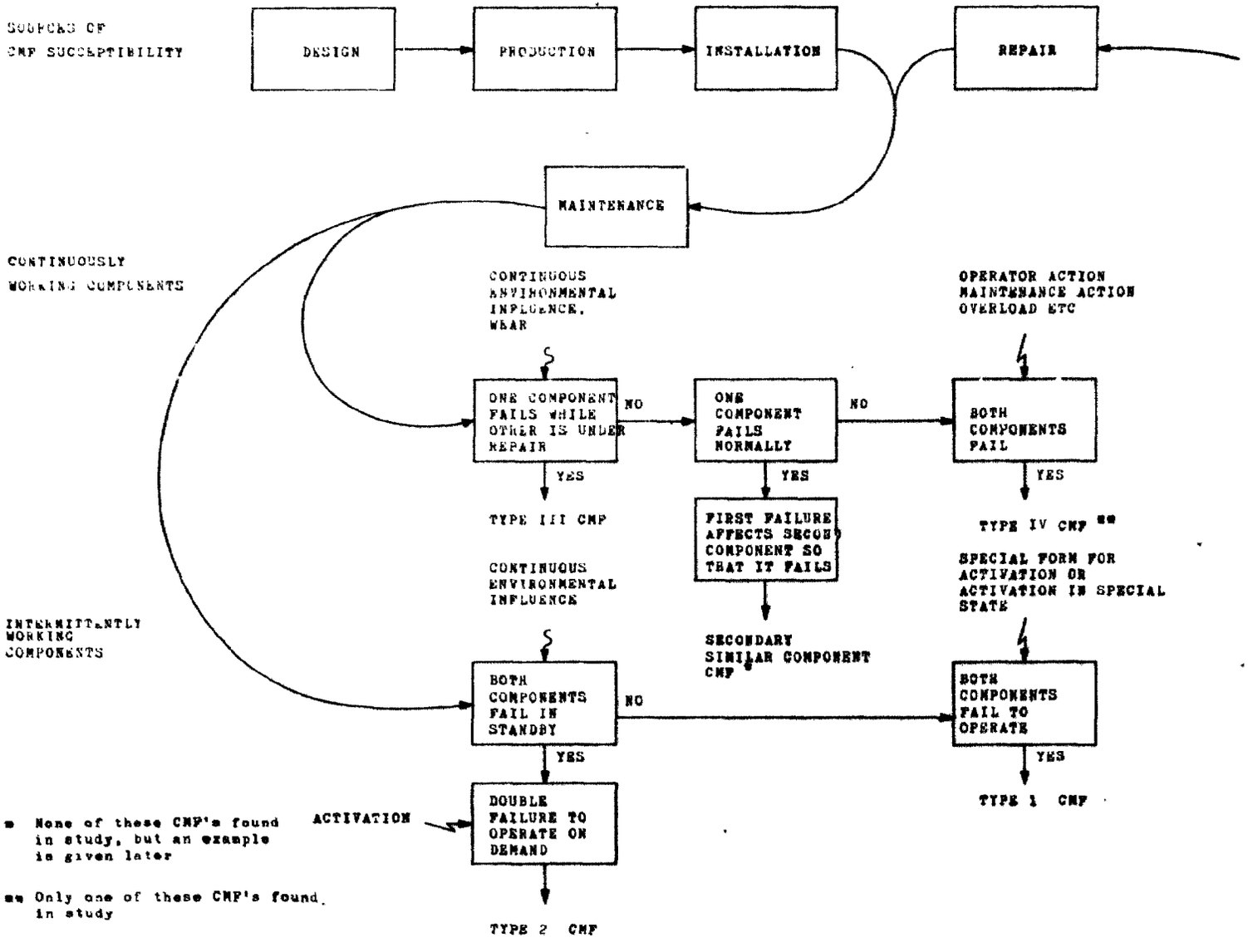
III Failures resulting from misadjustment or environmental effects on a group of continuously operating components, so that all fail shortly afterwards; or failures resulting from misoperation of a group of components; or consequent failures in general. This class corresponds to coupling type (d) above.

IV Failures arising from effects similar to those in class II but giving an unusually high failure rate in operation, so that one component fails while another is being repaired. (Only one instance of this type was found in the cases studied).

Note that the main practical difference between type I and type II coupled failures is that with type II, increasing testing frequency can reduce the probability of coupled failure.

Statistically coupled failures are those which affect several components simultaneously, in spite of the fact that, if the failures occurred separately, they would be regarded as "normal" random failures. In other words, any of the other coupled failure mechanisms may be present. Their presence is not however recognised directly, but only via their effect on system failure rates. The classes are similar to those for similar component coupled failures.

## SIMILAR COMPONENT COUPLED FAILURE




* None of these CMF's found in study, but an example is given later

** Only one of these CMF's found in study

## 3. EXAMPLES OF COUPLED FAILURE

The first eight of the following examples, intended to illustrate the classification of coupled failures, are taken from US Power Reactor abnormal occurrence reports. All were discovered during system testing, or had only limited safety consequences.

Other examples are taken from USAEC Reactor Operating Experiences reports.

1)

The main steam isolation valves, as they existed after the shutdown on January 31, 1970, leaked to such an extent that the reactor could not be pressurized to 20 psig by the service air system. Based on later measurements, it is estimated that this system can deliver approximately 9000 CFH to the reactor vessel in the manner in which it was piped up. It is believed that the air delivered to the reactor leaked past MS03B and MS04B causing a pressure build up in the down stream steam line and header piping due to an external force on MS03B caused by its hanger support and externally induced stresses on MS04B from its hanger and pedestal support. As the pressure built up in the steam header, the air leaked back through MS04A, which was under similar stresses to those on MS04B.

Docket 50-219 March 1970

A coupled failure of type I (intermittently operating component, revealed during testing). The failure is apparently caused by mechanical interaction of the components with their mountings.

2)

'Each diesel generator at Oyster Creek is equipped with one, 130-gallon fuel oil day tank, one main fuel oil pump which takes suction from the day tank, and two fuel oil transfer pumps which take suction from the 15,000-gallon main oil tank. The fuel oil level in the day tank is controlled by float switches located in the day tank and operate so that as fuel is consumed by the engine and the fuel level drops, a fuel transfer switch will activate the no. 1 fuel transfer pump to maintain the day tank level. If the fuel level continues to drop, another low level transfer switch will activate fuel transfer pump no. 2 and a local annunciator at the unit will indicate a fuel transfer fault.

The two fuel oil transfer pumps are operated by 230-volt, single-phase, capacitor start motors. Upon investigation it was found that both motor-starting switches were not making proper contact so that, at times, the pumps would run and at other times they would not. In this instance, neither the no. 1 pump nor the backup no. 2 pump started. As a result, the day tank went empty and the engine shut down.'

Docket 50-219 Jan 1972

This is probably a type I coupled failure.

3)

A plant shutdown had progressed to the point where, with electrical output at approximately 90 MWe, a transfer of station loads from the Auxiliary Transformer to the Startup Transformers was attempted. When a closing signal was applied to the S1A breaker, a loss of power occurred the the "1A" 4160V AC bus, which among other things caused two circulatory water pumps, three reactor recirculation pumps and the operating condensate and feedwater pumps to trip. Diesel Generator #1 started in the "Fast Start" mode, reenergizing the 4160V "1C" bus and the requisite safeguard power supplies. An attempt was made to start the B and C condensate pumps, but before either pump could be started, the reactor scrammed due to low water level. Automatic transfer to the S1B transformer was accomplished, but later in attempting to start a condensate pump powered from the "1B" 4160V bus, S1B tripped initiating the "Fast Start" sequence on Diesel Generator #2. The second CRD pump was started to assist in monitoring reactor water level which dropped to 9 feet above the active fuel. The reactor was isolated to prevent water inventory loss and the emergency condensers were initiated as needed to remove decay heat. The point at which reactor isolation occurs and the emergency cooling system is initiated was not reached.

CAUSE:

The problem was traced to an incorrect setting of the current transformer ratio matching taps for the C phase differential relay on both startup transformers. In attempting to either carry a sizeable load or start a large loud, a differential fault was sensed, tripping the output breakers.

Docket 50-219-319

A type I coupled failure involving a sequence of switchings from one redundant component to another.

4)

**On March 14, 1971 at approximately 2:55 P.M. an incident occurred at the H. B. Robinson Unit No. 2 that led to the failure of the turbine. After a reactor trip and subsequent turbine trip, lubricating oil flow was lost to the turbine and generator bearings. The rotor came to rest in the abnormally short time of approximately 17 minutes and seized in several failed bearings.**

**Assessment of the damage indicated that all eight turbine and generator bearings had suffered some damage. Bearings 4 and 5, between the two low pressure turbines, failed to the extent that molten babbit flowed through the bearings.**

**During the reactor shutdown, seal flow was interrupted to two reactor coolant pumps for approximately one minute. Subsequent investigation indicated the shaft for "A" reactor coolant pump may have been distorted by uneven heating. This pump has been disassembled and a new shaft is being installed. The seal on "C" reactor coolant pump will be disassembled for inspection before the unit is returned to service.'**

Docket 50-261-57

A type I coupled failure, resulting from a cascade failure.

In the following pages, the sequence of events in this occurrence are quoted, to give some idea of the complexity in some cascade failures.

SEQUENCE OF EVENTS:

The unit was on the line carrying a load of 615 MWe as directed by the system load dispatcher. All plant conditions were normal. The operating staff was conducting the weekly routine checkoff of plant equipment.

8:30 A.M. Auxiliary Operator checked battery room and noted all indications normal in process of completing the shift Auxiliary Operator check-off list.

10:30 A.M. Auxiliary Operator started DC emergency oil pump, fed from "A" battery bus, for routine two (2) hour test run. This pump was not stopped as planned at 12:30 P.M. because the Auxiliary Operator became involved in other routine duties. All conditions remained normal until shortly before the reactor trip. One momentary alarm was received on "B" battery charger trouble annunciator. The alarm cleared immediately and no further trouble was experienced on "B" battery or battery charger.

2:49 P.M. The plant computer failed. Subsequent investigation indicated the failure was due to low DC voltage fed from battery bus "A".

2:50 P.M. The Control Operator observed reactor trip breaker "A" indication light was out and the Shift Foreman was notified. The bulb was changed with no success. Several other lights on RTGB were observed to be out. The Shift Foreman and Control Operator suspected instrument bus (AC) trouble. I & C technician assistance was summoned and Shift Foreman proceeded to check out MCC-5 and MCC-6 and all instrument busses for failure.

2:52 P.M. Received reactor coolant pumps thermal barrier cooling water low flow alarm. Outlet isolation valve 735 (air operated) closed on low DC control voltage. RTGB valve position indication also lost.

2:55 P.M. Received reactor trip due to low voltage on DC trip coils on reactor trip breakers. Reactor trip initiated turbine trip. No battery charger alarms were received.

2:56 P.M. Received generator lockout (one minute time delay) due to OCB closed and stop valves closed. A portion of the control room lights were lost. 4KV bus 4 switched to start-up transformer properly leaving 4KV bus 3 and 4 on start-up transformer. 4KV busses 1 and 2 were lost because DC control voltage on "A" battery was too low to close breaker

52/12 and put these busses on the start-up transformer. "A" diesel started properly due to loss of E-1 bus voltage. Diesel supply breaker 178 to E-1 bus did not close because of low DC control voltage from "A" battery.

The Shift Foreman and several other individuals while checking on 4KV voltage found no DC control voltage on several breakers. The batteries were checked immediately and "A" battery was found with 60 volts and "0" amps. All breakers on "A" battery bus were closed. The AC supply from MCC-5 to the "A" battery charger was lost when 4KV busses 1 and 2 were lost.

It should be noted that the battery chargers are rated at 300 amps with a current limiting device set at approximately 375 amps. It has been reported that the normal DC load on the "A" bus is approximately 150 amps. Assuming a 350 amp load imposed by the DC emergency oil pump, the load on the DC bus could have been as high as 500 amps. This would have imposed a minimum discharge rate on the "A" battery of at least 125 and possibly as much as 200 amps. A 200 amp discharge rate will lower battery voltage to 105V DC in approximately four hours assuming a fully charged battery initially.

3:00 P.M. The "B" charging pump was lost when E-1 voltage was lost. The "C" charging pump was started immediately to re-establish seals and charging flow. The seal leak-off temperature on reactor coolant pumps "A" and "C" rose sharply as indicated.

<u>#A RCP</u>

Recorder Point No. 1 - Seal leakoff 300°F.
Recorder Point No. 2 - Upper thrust 300°F.
Recorder Point No. 7 - Pump bearing is 280°F.

<u>#B RCP</u>

Recorder Point No. 15 - Pump bearing is 230°F.

<u>#C RCP</u>

Recorder Point No. 17 - Seal leakoff 300°F.
Recorder Point No. 23 - Pump bearing 230°F.

"A" and "C" pumps tripped when 4KV busses 1 and 2 were lost. The seal flow on "A" and "C" pumps decreased to zero. "B" pump continued to run with normal temperature and seal flow. Charging flow was lost for less than one minute.

The volume control tank had no level indicated. Operator switched to refueling water storage tank for supply to re-establish volume control tank for supply to re-establish volume control tank level. Switched back to normal lineup after 30 inches indicated in volume control tank.

A safety injection signal was activated due to instrumentation power supply failure. Pressurizer level remained above 20% and pressure above 2000 psig. All safety injection equipment except that from E-1 bus operated satisfactorily.

Operator observed turning gear oil pump and emergency DC oil pump lights were out.

3:12 P.M. The turbine rolled to a stop approximately 17 minutes after the turbine trip. Condenser vacuum was maintained. The AC turbine gear oil pump was not operable due to loss of MCC-5 power supply; i.e., loss of 4KV bus 1 and inability of diesel breaker 17B to close. The DC emergency oil pump was not operable due to low voltage on "A" battery.

3:20 P.M. The battery bus tie was closed and "A" battery voltage immediately increased to 125 volts. Breaker 15B closed re-establishing voltage on E-1 from "A" diesel. The Control Operator closed breaker 52/12 and picked up 4KV busses 1 and 2 from the start-up transformer. The Control Operator re-established power to 480V bus 1 via station service transformer "A". The turning gear oil pump started when E-1 power was re-established. The generator oil lift pump started and the turning gear engaged attempting to roll the turbine. The turbine would not turn and the turning gear motor began smoking heavily. The turning gear motor was manually tripped. Unsuccessful attempts were made to roll the turbine manually and with an air drive motor. Oil was pouring from the No. 5 turbine bearing. All attempts to roll the turbine were unsuccessful.

Condenser vacuum and steam seals were maintained on the unit and steam dump continued to the condenser.

Restoration of DC power provided for opening of valve 735 to restore reactor coolant pump thermal barrier flow.

3:25 P.M. Restored normal letdown from reactor coolant system.

Approximately five (5) minutes after restoring power to normal, MCC-6 tripped. Operator was unable to close breaker. The control fuses were replaced and the breaker then closed properly.

3:30 P.M. Turning gear oil and lift pump were secured due to oil leakage from No. 5 turbine bearing.

With the reactor in a safe condition, assessment of the turbine damage commenced.

The incident was determined to have been initiated by the decrease in "A" battery voltage to the point where components supplied by the "A" DC bus could not function as designed. Several factors contributed to the loss of voltage on "A" DC bus and the failure to detect this decrease in voltage.

1. The DC emergency oil pump was operating from the "A" DC bus. This resulted in an unanticipated discharge of the "A" battery. Due to personnel error, this pump was left operating and not shutdown after the scheduled two hour test.

   Operating procedures and operator training are being revieved to insure that unsatisfactory conditions are corrected.

2. No alarm is provided to warn the Control Operator of low DC bus voltage. The installation of suitable alarms is being investigated.

3. The AC oil pump is currently fed off of MCC-5. With the loss of E-1 voltage, MCC-5 is without a power supply. The possibility of changing the AC oil pump power supply to MCC-6 is being investigated in order to provide a completely redundant back-up lubricating oil supply to the turbine.

5)

On July 9, 1973, while operating at 94% power, "B" Safety Injection Pump tripped upon initiation of a manual start for a routine periodic test. Subsequent checks of "A" and "C" pumps resulted in the tripping of "C" pump upon starting. This condition was discovered at approximately 0900 hours while attempting to supply makeup water to the Safety Injection System accumulators using "B" Safety Injection Pump. An investigation of the incident revealed that the pump trips were the result of the instantaneous overcurrent trips on the pump breakers being set at their minimum value. Further investigation by Westinghouse service personnel verified that the actual setting on the trip devices for "B" and "C" pumps was approximately 100 amperes below the intended setting. The instantaneous trip settings on these breakers were increased to approximately 750% of name plate rating, and the pumps were satisfactorily tested and returned to service.

Docket 50-261-226

A type 1 coupled failure arising from design or installation error.

6)

IN ACCORDANCE WITH SECTION 6.6.2 OF THE TECHNICAL SPECIFICATION, THE FOLLOWING ABNORMAL OCCURANCE IS REPORTED:
AT 1430 HOURS ON 6-5-73, WHILE INVESTIGATING AND ABNORMAL INDICATION ON THE NARROW RANGE CONTAINMENT PRESSURE INDICATUR, IT WAS FOUND THAT 3 3/8 INCH VENT VALVES ON THE PRESSURE SENSING LINE TO ALL CONTAINMENT PRESSURE TRANSMITTERS WERE OPEN. THIS RESULTED IN ERRONEOUS SIGNALS TO PT'S 950, 951, 952, 953, 954, AND 955, WHICH SUPPLY INPUTS TO RTGB INDICATURS AND SAFEGUARD RACKS.

Docket 50-261-186

A type I coupled failure, presumably arising from an operator or procedural error.

7)

On Thursday, August 31, 1972, an inspection of the four RHR pump minimum flow protection flow switches for actuator paddle integrity was performed. The inspection revealed that a large piece of the paddle on No. 13 RHR pump flow switch and a small piece of the paddle on No. 11 RHR pump flow switch had broken off and were presumably carried down the associated RHR lines with flow."

Docket 50-263-153

A type II coupled failure presumably arising from a design error ( see Taylor (1974) for a definition of design error).

8)

At 1930 hours on June 17, 1972, the two series-installed air operated primary containment sample return isolation valves, 8501-3A and 8501-3B, failed to close during the quarterly testing required by Section 4.7.D.1.C.(1) of the Technical Specifications. Both valves were last satisfactorily tested on April 30, 1972.

Investigation of the valves verified that the control signals were properly de-energizing the valve solenoids and thereby bleeding the air off the air operator diaphragms. Visual observation indicated that the problem was physical binding within the valves.

Satisfaction of Section 3.7.D.2 of the Technical Specifications was achieved by closing a manual valve, 2-9201-500, located between the air operated valves and the primary containment.

Repairs to both valves were effected on June 19, 1972, by loosening the packing nuts and lubricating the valve shafts. The valves were operated several times from the control room, the packing nuts readjusted, and then the valves were operated several times again. After this switching both valves operated satisfactorily.

Docket 50-237-242

This is probably a type II coupled failure. Valve sticking presumably arose by drying out of lubrication, which is a slow process. Increasing inspection or servicing frequency could therefore have reduced coupled failure probability.

9)

During a hot shutdown of Unit 1 of the Zion Station, reactor coolant loop B was isolated, reactor coolant pump 1B was secured, and the B main steam isolation valve (MSIV) was subsequently closed due to a malfunction of the MSIV closure circuit. Since loop B was isolated from the steam generator, the steam temperature dropped. This caused pressure in this loop, $P_4$, to drop below that of loops A, C and D whose pressure values are designated as $P_1$, $P_2$ and $P_3$ respectively in Figure 1, the "As Built" wiring diagram.

The pressure drop in loop $P_4$ caused bistables 534A, 516C and 525A in the circuit logic to trip, producing half trips on three of the four protection channels related to loops A, C and D. Since a 2/3 logic is required, no safety injection trip signal for loop B was received.

As seen in Figure 2, bistables 534B, 516D and 525B would have tripped if the circuit logic had been wired correctly, producing the appropriate safety injection signal. However, even with the appropriate signal, actual safety injection would not have occurred, nor should have it occurred based on the design of the circuit, because all the loop isolation valves were closed.

An investigation by Commonwealth Edison personnel revealed that wires feeding the input signals to the dual comparators (514A/B, 534A/B, 515A/B, 525A/B, 516C/D and 526C/D) were wired in reverse from what they should have been for proper operation. This made a portion of the safety injection system initiation circuit inoperable.

R.O.E. 1975

A type I coupled failure arising from an error on a wiring diagram. It is often difficult to decide in the case of wiring errors, whether there are several separate channel errors, or one error at the system level.

Common Mode Failure of Local Power Range Monitors

10) **During the startup of Unit 1 of the Millstone Nuclear Power Station in September 1972, the plant had reached operational temperature and pressure, with the reactor power at 100 MW(t). When the operator noted an indication that the resins in one of the demineralizers were becoming depleted, he switched a second demineralizer into service. Since only condensate was being recirculated and no addition to the reactor coolant was necessary at the time, the operator proceeded with the startup. Half an hour later, high conductivity of the feedwater was noted, and the operator initiated a deliberate reactor shutdown. Ten minutes after reactor shutdown was begun, resins in both condensate demineralizers were completely depleted. An hour later, the operations supervisor ordered the reactor to be scrammed manually because of excessive chlorides in the primary system. The main steam line isolation valves were shut and the isolation condenser was placed in service to continue cooldown of the plant.**

About 30 minutes after the isolation condenser was placed into service, the first LPRM failed. Within the next 24 hours, all of the LPRM's had failed.

Of the 120 failed detectors, 116 showed low detector-to-cable resistance, indicating that the seal weld on the detector-to-cable shields had failed. This was substantiated by the upscale failures of the detectors, indicating very low resistance between the detector signal wire and the cable shield. Subsequent metallographic investigations revealed that chloride stress corrosion had caused the failures. No significant indications were obtained from dye-penetrant testing of the LPRM cables. This led to the conclusion that the route for entry of moisture into the cables was provided through the cable collars, through the chamber fill tubes, or through both paths.

The source of the moisture and high chloride content in the reactor coolant was in-leakage of about 17 gpm of seawater into the hot wells of the main condensers through leaking condenser tubes. The resulting chloride concentration in the reactor coolant caused the demineralizer resins to become depleted rapidly and resulted in rapid buildup of chloride concentration in the reactor cooling system.

All the LPRM detectors were replaced while the plant was shut down for maintenance and cleanup of the affected systems.

To prevent recurrence of this type of event, all 40,000 aluminum-brass condenser tubes were replaced with copper-nickel tubes to provide better resistance to chloride corrosion attack. Also, instrumentation was added to monitor condenser water chemistry.

Procedures for reactor operation have been changed and additional technical specifications have been effected.

R.O.E. August 1973

A type III coupled failure.

11)

UNCOUPLED CONTROL RODS

During startup of Unit No. 1 of the Dresden Nuclear Power Station after a 1973 fall refueling outage, instruments did not verify that four control rods were properly coupled to their control rod drives (CRD's), so each affected control rod was fully inserted and the control rod drive electrically disarmed and removed from service. After reactor shutdown on August 31, 1974, it was determined that each of the suspected control rods had not been properly coupled in the 1973 refueling outage; they were found lodged between their associated fuel assemblies. No damage was noted.

It was concluded the control rods became uncoupled because procedures followed during the refueling outage were not performed in the proper sequence. Although a satisfactory pull test had been completed for each of the eighty control rods in the core, the test was completed prior to loading the four associated fuel assemblies. As a result, it was possible for a control rod to rotate 90° and become unlatched from the control rod drive coupling spud.

Power Reactor
Current Events 1974

A type I coupled failure.

12) Circumstances

On October 20, 1973, a turbine vibration alarm was annunciated on the control panel of Unit 1 of the San Onofre Nuclear Generating Station. One minute later, saltwater intrusion was indicated by high conductivity alarms from monitors located in the condenser. An investigation to determine the cause of both alarms was started immediately. Approximately forty minutes after the turbine vibration alarm, a systematic load decrease was begun; and one hour and fifteen minutes after the alarm was received, the plant was removed from the line and the plant load was switched to the auxiliary transformers.

Approximately eight minutes after the plant load had been switched, a noload turbine trip alarm was received, although the turbine had been removed from service. The trip alarm caused the turbine stop valves to close. During removal of the plant from the line, the operator had failed to switch the feedwater control system to manual. This sequence of events caused the feedwater regulating valves to open automatically to 80% of full open because the average primary coolant temperature was greater than 540 degrees F. The switching of the feedwater control from automatic to manual is a standard requirement for a routine shutdown.

The opening of the feedwater valves allowed the average temperature and pressure of the reactor coolant to drop rapidly. The water level in the steam generators was observed to be increasing rapidly, the pressurizer level had decreased to 10% and the letdown valve had closed. The rapid filling of the steam generators resulted in a rapid cooldown and decrease in the total pressure of the primary system.

The primary system controls were placed in the manual mode and one of the control rod banks was pulled to mitigate further drops in primary system pressure and temperature. Feedwater control was also changed to the manual mode, the feedwater control valves were closed, and the feedwater block valves were manually closed.

This rapid cooldown and decrease in total primary system pressure resulted in the automatic initiation of the safety injection system (SIS). Although no Safety Limits or other Technical Specifications had been exceeded, approximately 1300 gallons of borated water from the refueling tank entered the primary system through the charging pump. The borated water did not enter through the safety injection lines because the system pressure still had not dropped below the actuation point.

The failures of the valve motor operator and pipe support equipment were attributed to a water hammer that occurred in the SIS loop caused by trapped air accumulated by normal inleakage. The motion of the piping generated sufficient force to shear the turnbuckle-type hanger and to cause the tensile failure of four bolts (0.17-inch diameter) that hold the casting of the valve motor operator to the safety injection valve. The failure of these four bolts resulted in the motor casing, stator, and end bell dropping from their mountings.

ROE 74-15

A cascade coupled failure.

## 4. DEFINITION OF COUPLED FAILURE

A simple practical definition of coupled failure is readily given

> "coupled failures are simultaneous failures of several components as a result of a common cause".

To be useful in all cases this definition must be further specified. What is a "simultaneous failure"? The only reasonable definition which this author could obtain, is that by "simultaneous failure" we mean that several components are in a failed state at the same time.

Whether two failures are considered to occur or just one, depends on the degree to which a system is divided into components. For example, if two contacts on the same switch fail because they are both dirty, is this a case of coupled failure or a single failure?.

A reasonable criterion for dividing a system into components was presented in the Rasmussen report (WASH 1400, Draft 1974):

> "[In the study]
>
> The analyses were generally developed to a component level of resolution where a component refers to a hardware entity for which failure data are generally available. For example, more data are available for a diesel-generator than for the diesel, generator and auxiliaries taken individually; therefore, a diesel-generator would not ordinarily be analyzed into its constituent parts. In some cases, however, more in-depth analysis was required solely to determine the logical relationship between various inputs to a component. For example, the interlocks between two air circuit breakers may not be apparent unless the circuit breakers close and trip circuits considered in the evaluation".

For our purposes, the principle can be expressed more shortly. A system is divided into components to a level where failure data are generally available, and is then further divided, if two parts of a component have different functions.

In recording failure data, a coupled failure is considered to have occurred if two components (that is, units for which failure

data is generally collected) are in a failed state simultaneously. In addition if two parts of a single component, each of which serves a different function, fail, then a coupled failure is recorded.

This definition raises another question; should all simultaneous failures arising from a common cause be regarded as coupled failures; or only those failures occurring in redundant components. In this note, all simultaneous failures arising from a common cause are regarded as coupled failures irrespective of whether the failed components are redundant.

To make the definition complete, "failure" is defined. A "failure occurs" when a component cannot operate according to its specification when called on to do so, or when a component ceases to operate according to its specification while it is still called on to do so. A component is in a failed state, if it is unable to operate as specified.

The definition of coupled failure given above, when qualified as indicated, is adequate, provided that the failure cause on trigger acts only over short period of time, or can be regarded as an instantaneous event. The definition is also practical, in such cases. It is easy to tell whether a coupled failure has occurred or not, in all cases where either the failure cause is known, or failure modes are identical.

A problem arises with this definition, however, if the cause of failure is a phenomenon which works slowly and continuously. The problem is best illustrated by an example.

Consider the case of two filament lamps, continuously operating subject to vibration. If high levels of vibration occur occasionally, the lamps may fail at times which are very close to each other (within one second). One could normally say that the failures are coupled. At some lower level of vibration (still periodic, or occasional) there may be some strong correlation between failure times. There will be some vibration level which is "normal" but even that level will be subject to "normal" variations. As a result, even normal failure rates will imply some correlation between failure times.

In practice, this kind of failure behaviour is important when components with limited lifetimes are used; in corrosion failures; and in failures arising from occasional environment extremes.

As a result of this kind of problem, it becomes impossible to

distinguish between coupled and independent failures in many cases, if the phenomenological definition given above is used.

As an alternative to the definition above, which is in terms of failure causes, one can look more directly at the purpose of collecting coupled failure data, or of interest in coupled failure. This interest generally arises from the fact that reliability or availability of redundant systems is reduced if there is a possibility of coupling of failures.

A "coupling coefficient" can be derived for the probability of failure of two components, A and B as

$$C = \frac{P\ (A,B)}{P(A)\ P(B)}$$

Here P (A,B) is the probability that both components fail when a particular coupling mechanism is present, P(A) and P(B) are the failure probabilities when the coupling mechanism is not present, or when it affects the two components with independent probability.

In general, there will be several possible coupling coefficients, depending on whether the probabilities used are reliabilities, point availabilities, limiting availabilities etc. A possibility for coupled failure is said to exist, if a coupling coefficient is greater than one. Coupled failures are said to have occurred, if a mathematical model explaining the failure probability yields a coupling coefficient greater than one.

The reasoning here follows very closely that given in the Rasmussen Report (WASH 1400 Draft Appendix IV).

A subtle point concerns precisely which probabilities should be used for P(A) and P(B) in the formula given above. If failure probabilities observed in actual practice in the plant are used, then coupling effects due to design errors, poor quality component batches, etc. will not be relevant, and will not be reflected in the coupling coefficient. If a priori estimates for P(A), P(B) are used, then the coupling coefficient will reflect such coupling effects.

In a similar way, if P(A), P(B) and P(A,B) are point values, functions of time, then the coupling coefficient may vary with time, but it will not directly reflect the effects of "clustering" of failures in time. If, on the other hand, probability averages

over a period of time are used then the coupling effect of hazard rate vatiations with time (such as those caused by environmental effects) will be reflected directly in the coupling coefficient.

Difficulties in deciding whether a double (or multiple) failure is a coupled failure, in borderline cases, suggests the policy of not attempting such a classification. Instead the number of double or multiple component failures is recorded as a variable independent of the single failure rate for the component.

## 5. PROBABILITY OF COUPLED FAILURE - SOME SIMPLE MODELS

The probability models described here are for the case in which a reliability estimate is needed for some future system, or one for which little experience exists. Reliability data must then be based on laboratory tests, or experience from other plant. There will be a certain a priori uncertainty as to whether the situation in the plant is actually the same as in other plants or in the laboratory tests. In such cases coupling coefficients will be calculated using a priori failure probabilities, and these may well be different from the probabilities later observed.

In this section coupling coefficients and the ratio of double to single failures are calculated for several simple coupled failure situations.

The importance of the ratio of single to double failures, is that it is very difficult to obtain sufficient data to establish coupled failure rates. The ratio of double to single failures is a sensitive indicator of the relative importance of coupled failures.

**Example 1** **Probability of failure to operate for a type I coupled failure, for two components working in parallel**

Two components, chosen from the same production batch, and designed and installed in the same way, are activated in parallel. There is a certain probability that the kind of activation will be such as to cause failure, if the components are succeptible to a type I common failure mode. There is also a certain probability that a component will fail on activation, at random, by some non-coupled failure mechanism.

Let $P_S(A)$ = Probability that the batch from which component A is chosen, is succeptible to the type I common failure mode.

$P_T$ = Probability, for any particular activation, that it will trigger the coupled failure mode.

$P_N(A)$ = Probability that component A fails on activation, by some non-coupled failure mode.

Probability of failure for a single component system.

$$= P(A) = P_T\, P_S(A) + P_N(A) - P_T\, P_S(A)\, P_N(A)$$

$$\sim P_T\, P_S(A) + P_N(A) \quad \text{in most cases.}$$

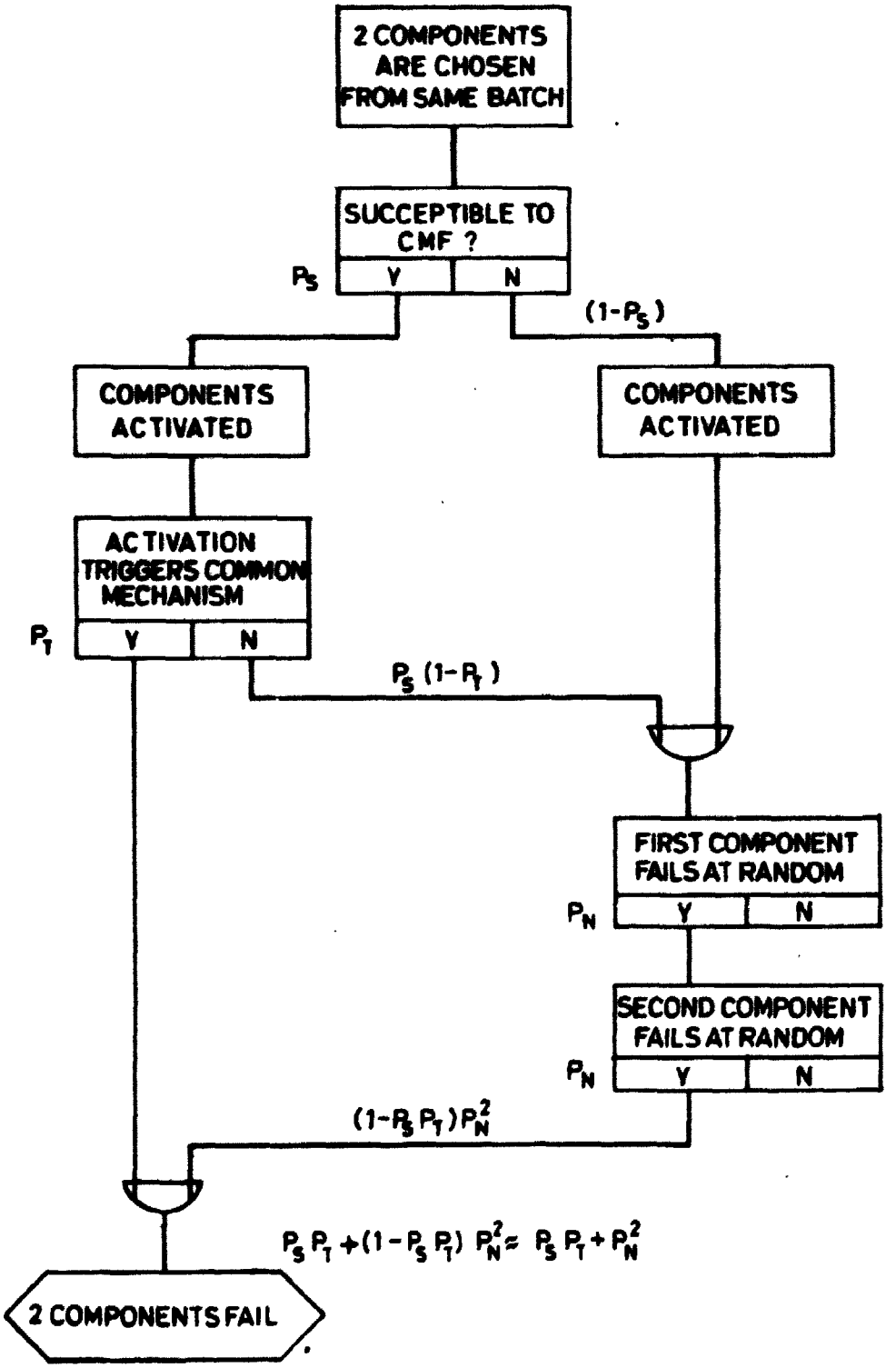



Fig. 3. Coupling via batch selection (design, manufacture, installation).

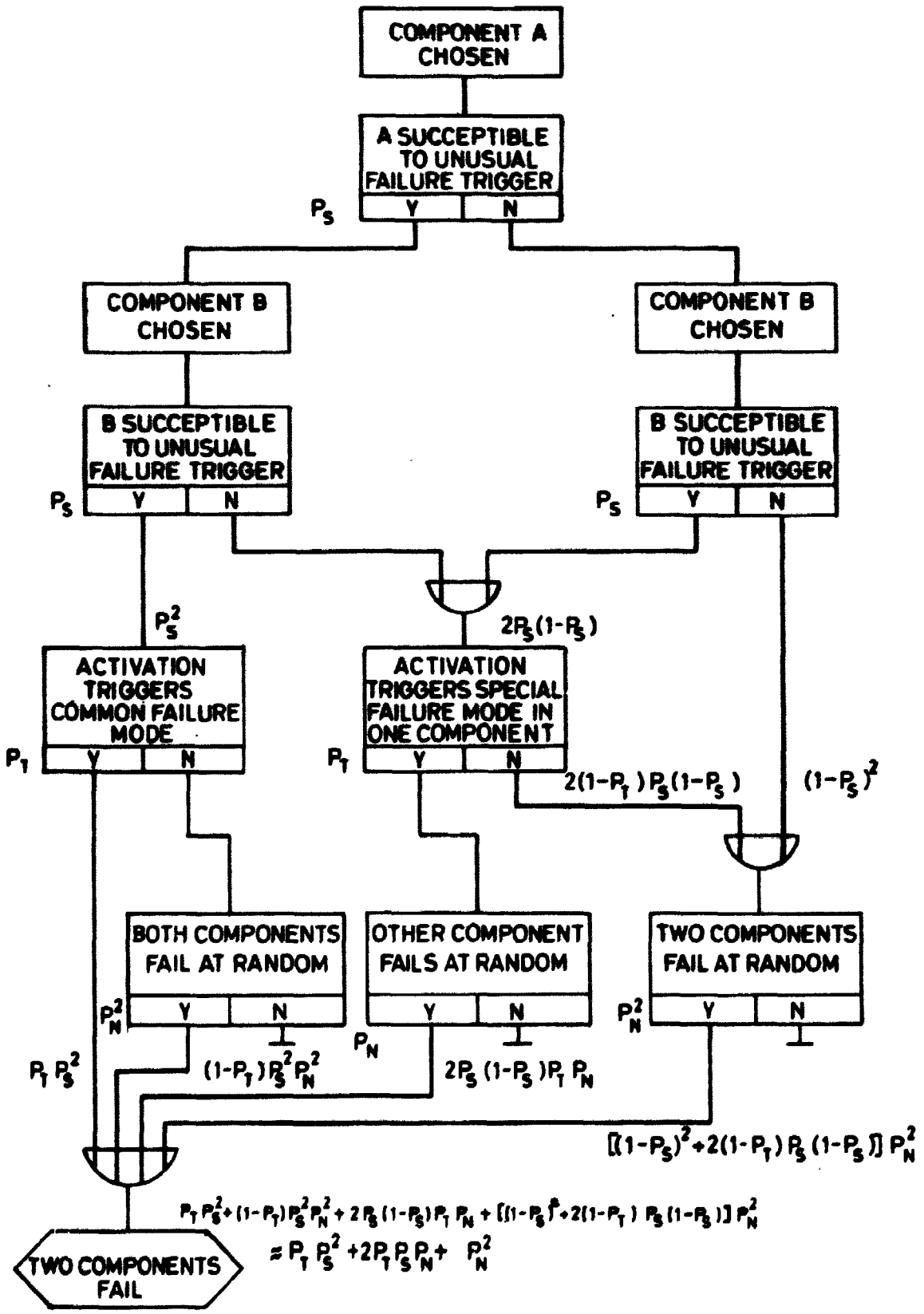



Fig. 4. Coupled failure is possible in two components but they are chosen separately.

Probability of double failure, for a two component system subject to coupled failure (similar components) is

$$P_C = P_S P_T + (1 - P_S P_T) P_N^2 \qquad \text{see figure 3}$$

$$= P_S P_T + P_N^2 - P_S P_T P_N^2$$

If $P_S P_T \ll 1$ $\qquad P_N \ll 1$

$$P_C \approx P_S P_T + P_N^2$$

Probability for double failure, for a two component system, with components not selected from the same batch, is

$$P = P_T P_S^2 + (1-P_T) P_S^2 P_N^2 + 2P_S (1-P_S) P_T P_N$$

$$+ \left[ (1-P_S)^2 + 2 (1-P_T) P_S (1-P_S) \right] P_N^2 \qquad \text{see figure 4}$$

$$= P_T P_S^2 + P_S^2 P_N^2 - P_T P_S^2 P_N^2$$

$$+ 2P_S P_T P_N - 2P_S^2 P_T P_N$$

$$+ P_N^2 - 2P_S P_N^2 + P_S^2 P_N^2$$

$$+ 2P_S P_N^2 - 2P_S^2 P_N^2$$

$$- 2P_T P_S P_N^2 + 2P_T P_S^2 P_N^2$$

$$= P_T P_S^2 (1+P_N^2) + 2P_S P_T P_N (1-P_S) - 2P_S P_T P_N^2 + P_N^2$$

Assuming $P_N \ll 1$ $\quad P_T P_S \ll 1$ $\quad P_N > P_T P_S$

$$P \approx P_T P_S^2 + 2P_T P_S P_N + P_N^2$$

Then the coupling coefficient for operational reliability of a two component system is

$$C_{OR,2} = \frac{P_C}{P} = \frac{P_T P_S + P_N^2 - P_S P_T P_N^2}{(P_T P_S^2 + P_T P_S^2 P_N^2 + 2P_T P_S P_N - 2P_T P_S^2 P_N + P_N^2 - 2P_T P_S P_N^2)}$$

$$\approx \frac{P_T P_S + P_N^2}{P_T P_S^2 + 2P_T P_S P_N + P_N^2}$$

In many practical cases, as will be seen later

$P_T P_S \approx 0.1 P_N$ and $P_N \approx 0.01$ (This would be typical for some kinds of motorized valves, for example)

Assume $P_T \approx 1$ then

$$C_{OR,2} \approx \frac{(0.1 + 0.01) P_N}{(0.01)P_N^2 + 2(0.1)P_N^2 + P_N^2}$$

$$\approx \frac{0.1}{1.21 \times 0.01}$$

$$\approx 8$$

Assume $P_S \approx 1$ then

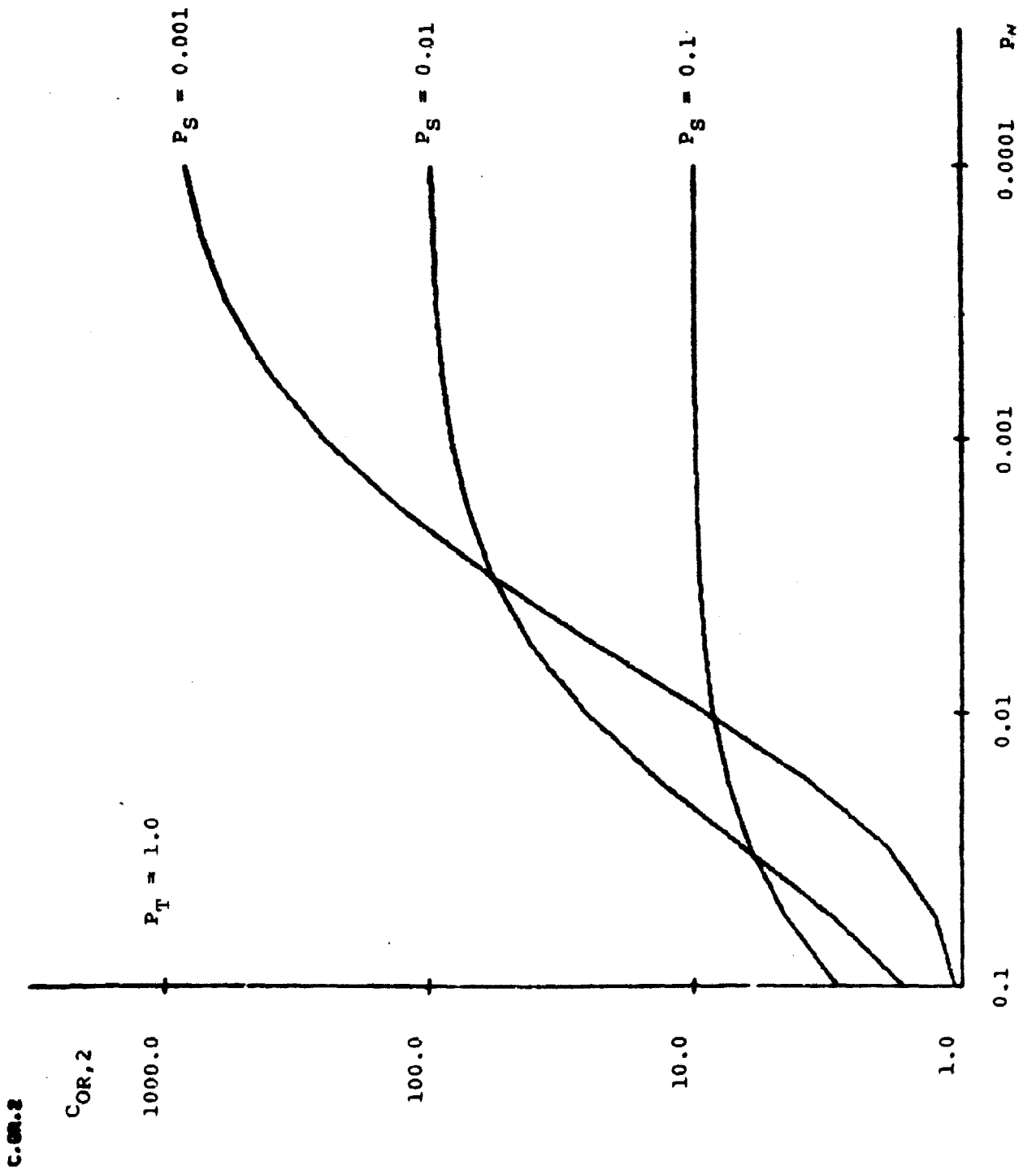
$$C_{OR,2} \approx \frac{0.1 P_N}{0.1 P_N^2 + 2(0.1) P_N^2 + P_N^2}$$

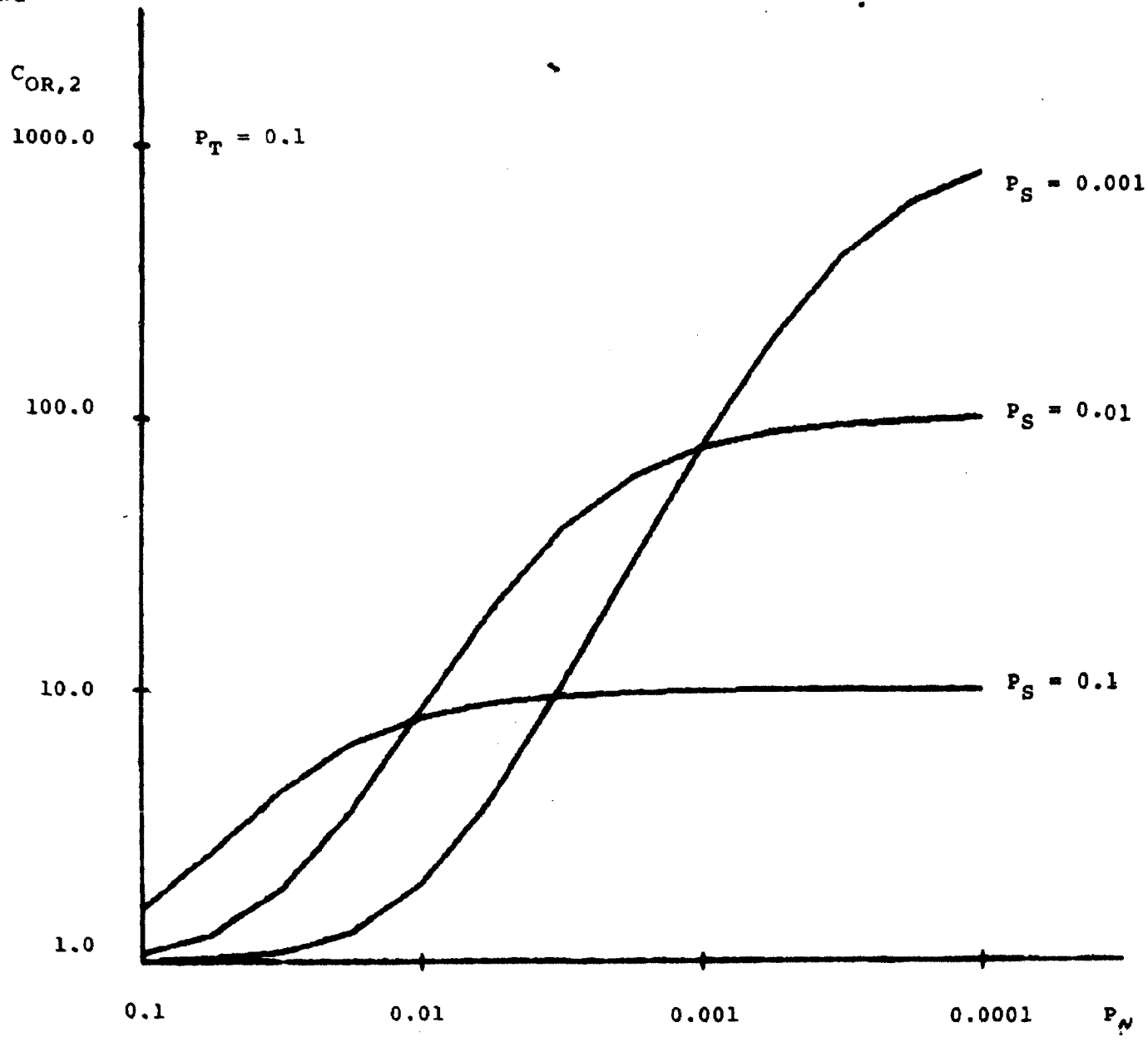
$$\approx \frac{0.1}{1.3 P_N} \approx 7$$

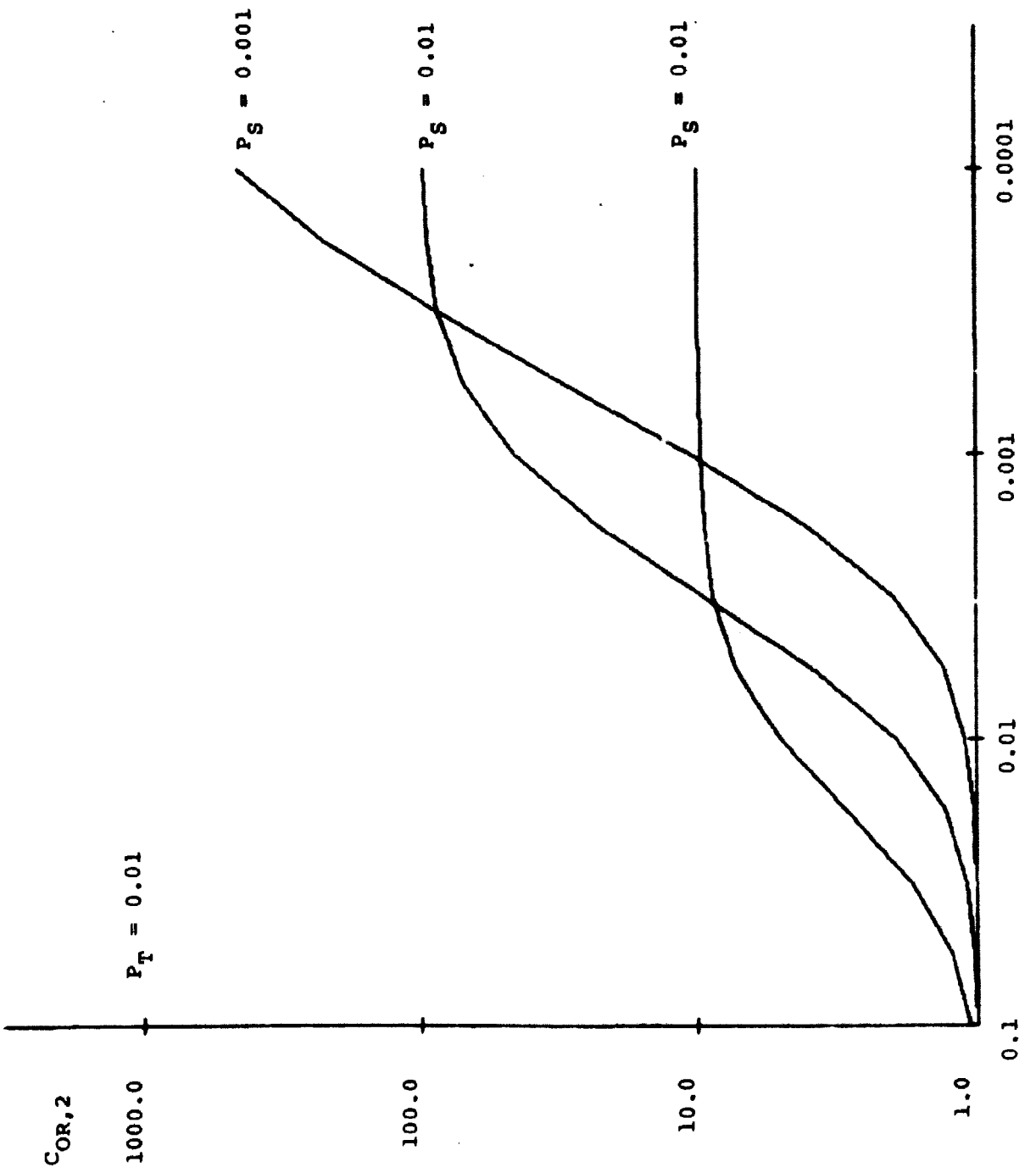
As the graphs of $C_{OR,2}$ on the following pages show, the value of the ratio of reliabilities, with and without coupling effects, is largest (worst) when $P_S$ is small and when $P_N$ is small. That is, when the components involved have a generally high reliability, but when there is a small proportion of unreliable components. The value of $C_{OR,2}$ is not very sensitive to $P_T$, provided $P_T > P_N$. Note that the value $P_T = 1.0$ is somewhat unrealistic - such failures would be easily detected during testing.

| $P_N$ | $C_{OR,2}$ | $P_S$ | $P_T$ | $P_N$ | $C_{OR,2}$ | $P_S$ | $P_T$ | $P_N$ | $C_{OR,2}$ | $P_S$ | $P_T$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.10000 | 3.01939 | 0.10000 | 1.00000 | 0.10000 | 1.57811 | 0.10000 | 0.10000 | 0.10000 | 1.07105 | 0.10000 | 0.01000 |
| 0.05623 | 4.53394 | 0.10000 | 1.00000 | 0.05623 | 2.56738 | 0.10000 | 0.10000 | 0.05623 | 1.23876 | 0.10000 | 0.01000 |
| 0.03162 | 6.11437 | 0.10000 | 1.00000 | 0.03162 | 4.30945 | 0.10000 | 0.10000 | 0.03162 | 1.73070 | 0.10000 | 0.01000 |
| 0.01778 | 7.45220 | 0.10000 | 1.00000 | 0.01778 | 6.32583 | 0.10000 | 0.10000 | 0.01778 | 2.93969 | 0.10000 | 0.01000 |
| 0.01000 | 8.42438 | 0.10000 | 1.00000 | 0.01000 | 7.90157 | 0.10000 | 0.10000 | 0.01000 | 5.04961 | 0.10000 | 0.01000 |
| 0.00562 | 9.06233 | 0.10000 | 1.00000 | 0.00562 | 8.85967 | 0.10000 | 0.10000 | 0.00562 | 7.20069 | 0.10000 | 0.01000 |
| 0.00316 | 9.45305 | 0.10000 | 1.00000 | 0.00316 | 9.38372 | 0.10000 | 0.10000 | 0.00316 | 8.73142 | 0.10000 | 0.01000 |
| 0.00178 | 9.66771 | 0.10000 | 1.00000 | 0.00178 | 9.66382 | 0.10000 | 0.10000 | 0.00178 | 9.43196 | 0.10000 | 0.01000 |
| 0.00100 | 9.52249 | 0.10000 | 1.00000 | 0.00100 | 9.81470 | 0.10000 | 0.10000 | 0.00100 | 9.73752 | 0.10000 | 0.01000 |
| 0.00056 | 9.89957 | 0.10000 | 1.00000 | 0.00056 | 9.89706 | 0.10000 | 0.10000 | 0.00056 | 9.87207 | 0.10000 | 0.01000 |
| 0.00032 | 9.94333 | 0.10000 | 1.00000 | 0.00032 | 9.94253 | 0.10000 | 0.10000 | 0.00032 | 9.93454 | 0.10000 | 0.01000 |
| 0.00018 | 9.96527 | 0.10000 | 1.00000 | 0.00018 | 9.96752 | 0.10000 | 0.10000 | 0.00018 | 9.96527 | 0.10000 | 0.01000 |
| 0.00010 | 9.98283 | 0.10000 | 1.00000 | 0.00010 | 9.98194 | 0.10000 | 0.10000 | 0.00010 | 9.98114 | 0.10000 | 0.01000 |
| 0.10000 | 1.67494 | 0.01000 | 1.00000 | 0.10000 | 1.07871 | 0.01000 | 0.10000 | 0.10000 | 1.00606 | 0.01000 | 0.01000 |
| 0.05623 | 3.04457 | 0.01000 | 1.00000 | 0.05623 | 1.26906 | 0.01000 | 0.10000 | 0.05623 | 1.02774 | 0.01000 | 0.01000 |
| 0.03162 | 6.44110 | 0.01000 | 1.00000 | 0.03162 | 1.56714 | 0.01000 | 0.10000 | 0.03162 | 1.09219 | 0.01000 | 0.01000 |
| 0.01778 | 13.53366 | 0.01000 | 1.00000 | 0.01778 | 3.64712 | 0.01000 | 0.10000 | 0.01778 | 1.29763 | 0.01000 | 0.01000 |
| 0.01000 | 25.53158 | 0.01000 | 1.00000 | 0.01000 | 6.46652 | 0.01000 | 0.10000 | 0.01000 | 1.94240 | 0.01000 | 0.01000 |
| 0.00562 | 41.39402 | 0.01000 | 1.00000 | 0.00562 | 19.57694 | 0.01000 | 0.10000 | 0.00562 | 3.91216 | 0.01000 | 0.01000 |
| 0.00316 | 58.05732 | 0.01000 | 1.00000 | 0.00316 | 38.48840 | 0.01000 | 0.10000 | 0.00316 | 9.46296 | 0.01000 | 0.01000 |
| 0.00178 | 72.32436 | 0.01000 | 1.00000 | 0.00178 | 60.15233 | 0.01000 | 0.10000 | 0.00178 | 22.85506 | 0.01000 | 0.01000 |
| 0.00100 | 82.50329 | 0.01000 | 1.00000 | 0.00100 | 77.13039 | 0.01000 | 0.10000 | 0.00100 | 45.95476 | 0.01000 | 0.01000 |
| 0.00056 | 89.73374 | 0.01000 | 1.00000 | 0.00056 | 87.52410 | 0.01000 | 0.10000 | 0.00056 | 70.27363 | 0.01000 | 0.01000 |
| 0.00032 | 94.02154 | 0.01000 | 1.00000 | 0.00032 | 93.24131 | 0.01000 | 0.10000 | 0.00032 | 86.10062 | 0.01000 | 0.01000 |
| 0.00018 | 96.57016 | 0.01000 | 1.00000 | 0.00018 | 96.38621 | 0.01000 | 0.10000 | 0.00018 | 93.76566 | 0.01000 | 0.01000 |
| 0.00010 | 98.04912 | 0.01000 | 1.00000 | 0.00010 | 97.96455 | 0.01000 | 0.10000 | 0.00010 | 97.11613 | 0.01000 | 0.01000 |
| 0.10000 | 1.37448 | 0.00100 | 1.00000 | 0.10000 | 1.28306 | 0.00100 | 0.10000 | 0.10000 | 1.06261 | 0.00100 | 0.01000 |
| 0.05623 | 1.27217 | 0.00100 | 1.00000 | 0.05623 | 1.28584 | 0.00100 | 0.10000 | 0.05623 | 1.06261 | 0.00100 | 0.01000 |
| 0.03162 | 1.85197 | 0.00100 | 1.00000 | 0.03162 | 1.09310 | 0.00100 | 0.10000 | 0.03162 | 1.08936 | 0.00100 | 0.01000 |
| 0.01778 | 3.73705 | 0.00100 | 1.00000 | 0.01778 | 1.30135 | 0.00100 | 0.10000 | 0.01778 | 1.03644 | 0.00100 | 0.01000 |
| 0.01000 | 9.16663 | 0.00100 | 1.00000 | 0.01000 | 1.95919 | 0.00100 | 0.10000 | 0.01000 | 1.09771 | 0.00100 | 0.01000 |
| 0.00562 | 23.55472 | 0.00100 | 1.00000 | 0.00562 | 4.00792 | 0.00100 | 0.10000 | 0.00562 | 1.31117 | 0.00100 | 0.01000 |
| 0.00316 | 55.35656 | 0.00100 | 1.00000 | 0.00316 | 10.25170 | 0.00100 | 0.10000 | 0.00316 | 1.96330 | 0.00100 | 0.01000 |
| 0.00178 | 136.12900 | 0.00100 | 1.00000 | 0.00178 | 26.52154 | 0.00100 | 0.10000 | 0.00178 | 4.10367 | 0.00100 | 0.01000 |
| 0.00100 | 250.50018 | 0.00100 | 1.00000 | 0.00100 | 77.71613 | 0.00100 | 0.10000 | 0.00100 | 10.66002 | 0.00100 | 0.01000 |
| 0.00056 | 410.10779 | 0.00100 | 1.00000 | 0.00056 | 189.80573 | 0.00100 | 0.10000 | 0.00056 | 30.57640 | 0.00100 | 0.01000 |
| 0.00032 | 577.55053 | 0.00100 | 1.00000 | 0.00032 | 368.37356 | 0.00100 | 0.10000 | 0.00032 | 86.84223 | 0.00100 | 0.01000 |
| 0.00018 | 721.07062 | 0.00100 | 1.00000 | 0.00018 | 596.46679 | 0.00100 | 0.10000 | 0.00018 | 222.06064 | 0.00100 | 0.01000 |
| 0.00010 | 826.80482 | 0.00100 | 1.00000 | 0.00010 | 769.43787 | 0.00100 | 0.10000 | 0.00010 | 455.04546 | 0.00100 | 0.01000 |

VALUES OF $C_{OR,2}$ FOR $P_N = 0.1 — 0.001$, $P_S = 0.1 — 0.001$ $P_T = 1.0 — 0.01$


$C_{OR,2}$
1000.0
100.0
10.0
1.0
0.1
$P_T$ = 1.0
$P_S$ = 0.001
$P_S$ = 0.01
$P_S$ = 0.1
0.1
0.01
0.001
0.0001
$P_W$


$C_{OR,2}$
1000.0
100.0
10.0
1.0
$P_T$ = 0.1
$P_S$ = 0.001
$P_S$ = 0.01
$P_S$ = 0.1
0.1
0.01
0.001
0.0001
$P_N$


$C_{OR,2}$
1000.0
100.0
10.0
1.0
0.1
$P_T$ = 0.01
$P_S$ = 0.001
$P_S$ = 0.01
$P_S$ = 0.01
0.0001
0.001
0.01

**Example 2** Components are selected from batches, all components in a batch having a constant hazard rate. But hazard rates vary from batch to batch. In the coupled case, components are chosen from the same batch. In the non-coupled case, components are chosen independently. After failure, components are repaired with meantime to repair completion $1/\mu$. (This case could represent type II failures with continuous monitoring of operational state, or type IV failures). The system considered has two redundant components.

Limiting unavailability for a single component = $\frac{\lambda}{\lambda + \mu}$ drawn from a batch with a single hazard rate.

The hazard rate distribution for the batches has two groups with hazard rates $\lambda_1, \lambda_2$. The probability of selection from a batch with hazard rate $\lambda_1$ is p.

The expected value of limiting availability for a single component, drawn from one of two batches

$$= \frac{p\ \lambda_1}{\lambda_1 + \mu} + \frac{(1-p)\ \lambda_2}{\lambda_2 + \mu}$$

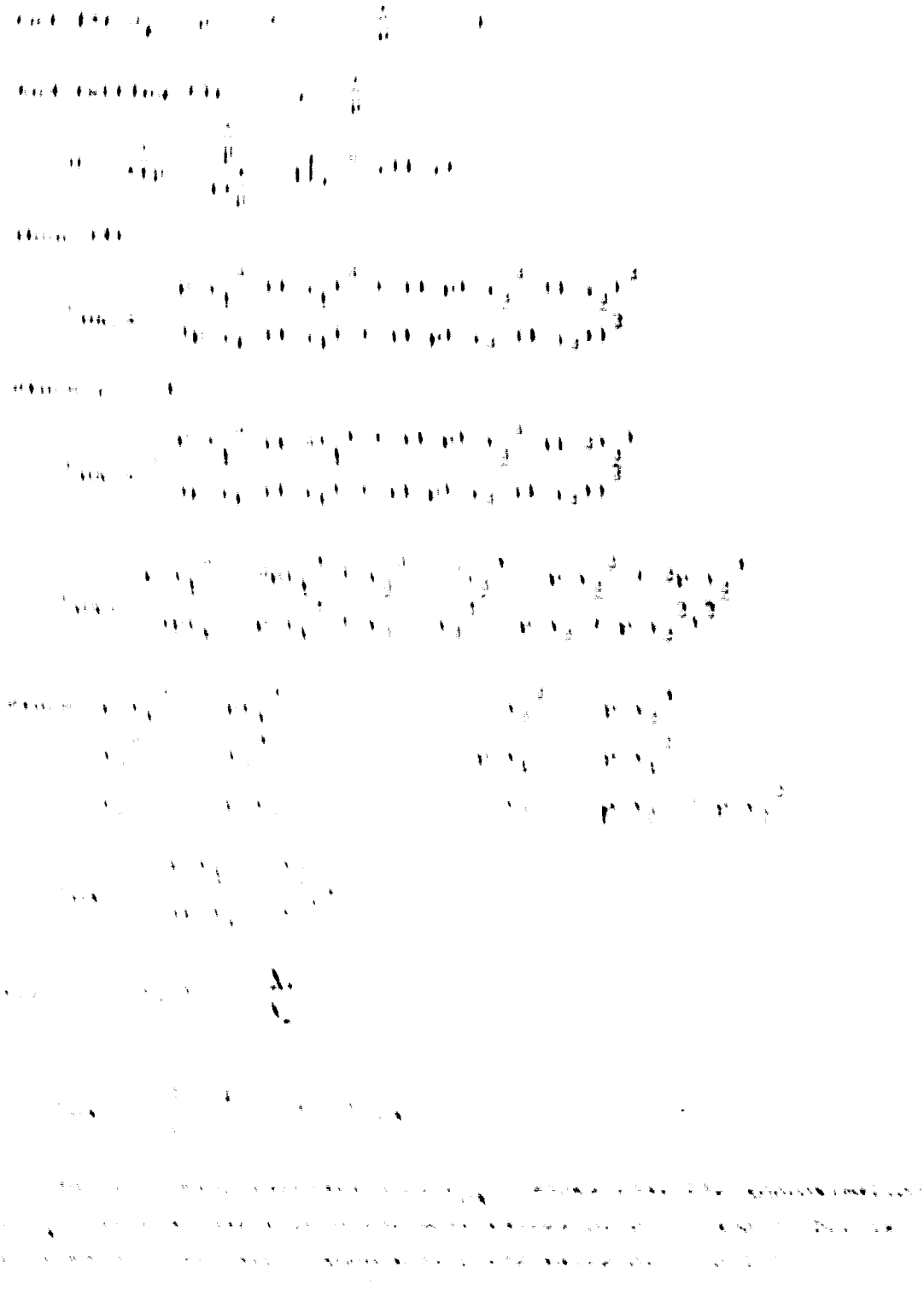
The coupling coefficient for limiting unavailability

$$C_{UA,2} = \frac{p\left(\frac{\lambda_1}{\lambda_1+\mu}\right)^2 + (1-p)\left(\frac{\lambda_2}{\lambda_2+\mu}\right)^2}{\left[p\left(\frac{\lambda_1}{\lambda_1+\mu}\right) + (1-p)\left(\frac{\lambda_2}{\lambda_2+\mu}\right)\right]^2}$$

if

(1) $\frac{\lambda_1}{\lambda_1+\mu} >> \frac{\lambda_2}{\lambda_2+\mu}$ and $p\ \frac{\lambda_1}{\lambda_1+\mu} \approx (1-p)\ \frac{\lambda_2}{\lambda_2+\mu}$

i.e. the poor batch is responsible for a reasonable proportion of all single failures, in spite of a small value of p,



The values tabulated are for

$\lambda_2 = 0.1\ \mu$ to $\lambda_2 = 0.00001\ \mu$

$\frac{\lambda_1}{\lambda_2} = 10.0$ to $\frac{\lambda_1}{\lambda_2} = 1000.0$

$p = 0.1$ to $p = 0.001$

**Ratio of unavailability with coupled failure to unavailability without**

| $\lambda_2$ | $C_{UA,2}$ | $C'_{UA,2}$ | $U_1 = C_{UA,2}$ | $U_2$ |
|---|---|---|---|---|
| LAMBDA1/LAMBDA2= | 10.0000 P= | 0.1000 M= | 1.0000 | |
| 0.10000 | 1.86683 | 2.75000 | 0.50000 | 0.09091 |
| 0.05623 | 2.20235 | 2.75000 | 0.35993 | 0.05324 |
| 0.03162 | 2.48422 | 2.75000 | 0.24025 | 0.03065 |
| 0.01778 | 2.68853 | 2.75000 | 0.15098 | 0.01747 |
| 0.01000 | 2.82250 | 2.75000 | 0.09091 | 0.00990 |
| 0.00562 | 2.90496 | 2.75000 | 0.05324 | 0.00559 |
| 0.00316 | 2.95381 | 2.75000 | 0.03065 | 0.00315 |
| 0.00178 | 2.98211 | 2.75000 | 0.01747 | 0.00178 |
| 0.00100 | 2.99830 | 2.75000 | 0.00990 | 0.00100 |
| 0.00056 | 3.00749 | 2.75000 | 0.00559 | 0.00056 |
| 0.00032 | 3.01269 | 2.75000 | 0.00315 | 0.00032 |
| 0.00018 | 3.01562 | 2.75000 | 0.00178 | 0.00018 |
| 0.00010 | 3.01727 | 2.75000 | 0.00100 | 0.00010 |
| 0.00006 | 3.01820 | 2.75000 | 0.00056 | 0.00006 |
| 0.00003 | 3.01872 | 2.75000 | 0.00032 | 0.00003 |
| 0.00002 | 3.01901 | 2.75000 | 0.00018 | 0.00002 |
| 0.00001 | 3.01918 | 2.75000 | 0.00010 | 0.00001 |
| LAMBDA1/LAMBDA2= | 100.0000 P= | 0.1000 M= | 1.0000 | |
| 0.10000 | 3.01939 | 8.27273 | 0.90909 | 0.09091 |
| 0.05623 | 4.23062 | 8.27273 | 0.84902 | 0.05324 |
| 0.03162 | 5.46068 | 8.27273 | 0.75975 | 0.03065 |
| 0.01778 | 6.48772 | 8.27273 | 0.64006 | 0.01747 |
| 0.01000 | 7.22901 | 8.27273 | 0.50000 | 0.00990 |
| 0.00562 | 7.71377 | 8.27273 | 0.35993 | 0.00559 |
| 0.00316 | 8.01163 | 8.27273 | 0.24025 | 0.00315 |
| 0.00178 | 8.18793 | 8.27273 | 0.15098 | 0.00178 |
| 0.00100 | 8.29000 | 8.27273 | 0.09091 | 0.00100 |
| 0.00056 | 8.34836 | 8.27273 | 0.05324 | 0.00056 |
| 0.00032 | 8.38148 | 8.27273 | 0.03065 | 0.00032 |
| 0.00018 | 8.40021 | 8.27273 | 0.01747 | 0.00018 |
| 0.00010 | 8.41077 | 8.27273 | 0.00990 | 0.00010 |
| 0.00006 | 8.41672 | 8.27273 | 0.00559 | 0.00006 |
| 0.00003 | 8.42007 | 8.27273 | 0.00315 | 0.00003 |
| 0.00002 | 8.42195 | 8.27273 | 0.00178 | 0.00002 |
| 0.00001 | 8.42301 | 8.27273 | 0.00100 | 0.00001 |
| LAMBDA1/LAMBDA2= | 1000.0 P= | 0.1000 M= | 1.0000 | |
| 0.10000 | 3.22543 | 9.80306 | 0.99010 | 0.09091 |
| 0.05623 | 4.63775 | 9.80306 | 0.98253 | 0.05324 |
| 0.03162 | 6.11437 | 9.80306 | 0.96935 | 0.03065 |
| 0.01778 | 7.37673 | 9.80306 | 0.94676 | 0.01747 |
| 0.01000 | 8.30315 | 9.80306 | 0.90909 | 0.00990 |
| 0.00562 | 8.91559 | 9.80306 | 0.84902 | 0.00559 |
| 0.00316 | 9.29444 | 9.80306 | 0.75975 | 0.00315 |
| 0.00178 | 9.51954 | 9.80306 | 0.64006 | 0.00178 |
| 0.00100 | 9.65018 | 9.80306 | 0.50000 | 0.00100 |
| 0.00056 | 9.72497 | 9.80306 | 0.35994 | 0.00056 |
| 0.00032 | 9.76745 | 9.80306 | 0.24025 | 0.00032 |
| 0.00018 | 9.79147 | 9.80306 | 0.15098 | 0.00018 |
| 0.00010 | 9.80503 | 9.80306 | 0.09091 | 0.00010 |
| 0.00006 | 9.81266 | 9.80306 | 0.05324 | 0.00006 |
| 0.00003 | 9.81696 | 9.80306 | 0.03065 | 0.00003 |
| 0.00002 | 9.81938 | 9.80306 | 0.01747 | 0.00002 |
| 0.00001 | 9.82074 | 9.80306 | 0.00990 | 0.00001 |

Ratio of unavailability with coupled failure to unavailability witnout

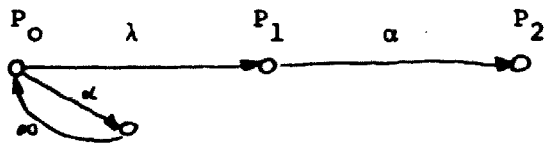
| $\lambda_2$ LAMBDA1/LAMBDA2= | $C_{UA,2}$ 10.0000 P= | $C'_{UA,2}$ 0.0100 $\mu$ = | $U_1 = C_{U1,2}$ 1.0000 | $U_2$ |
|---|---|---|---|---|
| 0.10000 | 1.18358 | 1.65289 | 0.50000 | 0.09091 |
| 0.05623 | 1.29371 | 1.65289 | 0.35993 | 0.05324 |
| 0.03162 | 1.40552 | 1.65289 | 0.24025 | 0.03065 |
| 0.01778 | 1.49886 | 1.65289 | 0.15098 | 0.01747 |
| 0.01000 | 1.56627 | 1.65289 | 0.09091 | 0.00990 |
| 0.00562 | 1.61034 | 1.65289 | 0.05324 | 0.00559 |
| 0.00316 | 1.63742 | 1.65289 | 0.03065 | 0.00315 |
| 0.00178 | 1.65345 | 1.65289 | 0.01747 | 0.00178 |
| 0.00100 | 1.66273 | 1.65289 | 0.00990 | 0.00100 |
| 0.00056 | 1.66803 | 1.65289 | 0.00559 | 0.00056 |
| 0.00032 | 1.67104 | 1.65289 | 0.00315 | 0.00032 |
| 0.00018 | 1.67275 | 1.65289 | 0.00178 | 0.00018 |
| 0.00010 | 1.67371 | 1.65289 | 0.00100 | 0.00010 |
| 0.00006 | 1.67425 | 1.65289 | 0.00056 | 0.00006 |
| 0.00003 | 1.67455 | 1.65289 | 0.00032 | 0.00003 |
| 0.00002 | 1.67472 | 1.65289 | 0.00018 | 0.00002 |
| 0.00001 | 1.67482 | 1.65289 | 0.00010 | 0.00001 |
| LAMBDA1/LAMBDA2= | 100.0000 P= | 0.0100 $\mu$ = | 1.0000 | |
| 0.10000 | 1.67494 | 25.25000 | 0.90909 | 0.09091 |
| 0.05623 | 2.67397 | 25.25000 | 0.84902 | 0.05324 |
| 0.03162 | 4.65517 | 25.25000 | 0.75975 | 0.03065 |
| 0.01778 | 7.83312 | 25.25000 | 0.64006 | 0.01747 |
| 0.01000 | 11.85333 | 25.25000 | 0.50000 | 0.00990 |
| 0.00562 | 15.89457 | 25.25000 | 0.35993 | 0.00559 |
| 0.00316 | 19.24321 | 25.25000 | 0.24025 | 0.00315 |
| 0.00178 | 21.64695 | 25.25000 | 0.15098 | 0.00178 |
| 0.00100 | 23.21330 | 25.25000 | 0.09091 | 0.00100 |
| 0.00056 | 24.17368 | 25.25000 | 0.05324 | 0.00056 |
| 0.00032 | 24.74134 | 25.25000 | 0.03065 | 0.00032 |
| 0.00018 | 25.06978 | 25.25000 | 0.01747 | 0.00018 |
| 0.00010 | 25.25747 | 25.25000 | 0.00990 | 0.00010 |
| 0.00006 | 25.36399 | 25.25000 | 0.00559 | 0.00006 |
| 0.00003 | 25.42419 | 25.25000 | 0.00315 | 0.00003 |
| 0.00002 | 25.45815 | 25.25000 | 0.00178 | 0.00002 |
| 0.00001 | 25.47727 | 25.25000 | 0.00100 | 0.00001 |
| LAMBDA1/LAMBDA2= | 1000.0 P= | 0.0100 $\mu$ = | 1.0000 | |
| 0.10000 | 1.80204 | 82.65289 | 0.99010 | 0.09091 |
| 0.05623 | 3.18633 | 82.65289 | 0.98253 | 0.05324 |
| 0.03162 | 6.44110 | 82.65289 | 0.96935 | 0.03065 |
| 0.01778 | 12.93444 | 82.65289 | 0.94676 | 0.01747 |
| 0.01000 | 23.42546 | 82.65289 | 0.90909 | 0.00990 |
| 0.00562 | 36.79715 | 82.65289 | 0.84902 | 0.00559 |
| 0.00316 | 50.33027 | 82.65289 | 0.75975 | 0.00315 |
| 0.00178 | 61.60402 | 82.65289 | 0.64006 | 0.00178 |
| 0.00100 | 69.72707 | 82.65289 | 0.50000 | 0.00100 |
| 0.00056 | 75.03314 | 82.65289 | 0.35994 | 0.00056 |
| 0.00032 | 78.29132 | 82.65289 | 0.24025 | 0.00032 |
| 0.00018 | 80.21889 | 82.65289 | 0.15098 | 0.00018 |
| 0.00010 | 81.33468 | 82.65289 | 0.09091 | 0.00010 |
| 0.00006 | 81.97253 | 82.65289 | 0.05324 | 0.00006 |
| 0.00003 | 82.33455 | 82.65289 | 0.03065 | 0.00003 |
| 0.00002 | 82.53921 | 82.65289 | 0.01747 | 0.00002 |
| 0.00001 | 82.65463 | 82.65289 | 0.00990 | 0.00001 |

Ratio of unavailability with coupled failure to unavailability without

| $\lambda_1/\lambda_2$ | $C_{UA,2}$ | $C'_{UA,2}$ | $U_1 = C_{UA,2}$ | $U_2$ |
|---|---|---|---|---|
| LAMBDA1/LAMBDA2= | 10.0000 P= | 0.0010 μ= | 1.0000 | |
| 0.10000 | 1.02005 | 1.07833 | 0.50000 | 0.09091 |
| 0.05623 | 1.03277 | 1.07833 | 0.35993 | 0.05324 |
| 0.03162 | 1.04608 | 1.07833 | 0.24025 | 0.03065 |
| 0.01778 | 1.05745 | 1.07833 | 0.15098 | 0.01747 |
| 0.01000 | 1.06579 | 1.07833 | 0.09091 | 0.00990 |
| 0.00562 | 1.07131 | 1.07833 | 0.05324 | 0.00559 |
| 0.00316 | 1.07472 | 1.07833 | 0.03065 | 0.00315 |
| 0.00178 | 1.07675 | 1.07833 | 0.01747 | 0.00178 |
| 0.00100 | 1.07793 | 1.07833 | 0.00990 | 0.00100 |
| 0.00056 | 1.07860 | 1.07833 | 0.00559 | 0.00056 |
| 0.00032 | 1.07899 | 1.07833 | 0.00315 | 0.00032 |
| 0.00018 | 1.07920 | 1.07833 | 0.00178 | 0.00018 |
| 0.00010 | 1.07932 | 1.07833 | 0.00100 | 0.00010 |
| 0.00006 | 1.07939 | 1.07833 | 0.00056 | 0.00006 |
| 0.00003 | 1.07943 | 1.07833 | 0.00032 | 0.00003 |
| 0.00002 | 1.07945 | 1.07833 | 0.00018 | 0.00002 |
| 0.00001 | 1.07947 | 1.07833 | 0.00010 | 0.00001 |
| LAMBDA1/LAMBDA2= | 100.0000 P= | 0.0010 μ = | 1.0000 | |
| 0.10000 | 1.07948 | 9.09091 | 0.90909 | 0.09091 |
| 0.05623 | 1.21666 | 9.09091 | 0.84902 | 0.05324 |
| 0.03162 | 1.53921 | 9.09091 | 0.75975 | 0.03065 |
| 0.01778 | 2.18269 | 9.09091 | 0.64006 | 0.01747 |
| 0.01000 | 3.22234 | 9.09091 | 0.50000 | 0.00990 |
| 0.00562 | 4.54746 | 9.09091 | 0.35993 | 0.00559 |
| 0.00316 | 5.88858 | 9.09091 | 0.24025 | 0.00315 |
| 0.00178 | 7.00580 | 9.09091 | 0.15098 | 0.00178 |
| 0.00100 | 7.81079 | 9.09091 | 0.09091 | 0.00100 |
| 0.00056 | 8.33662 | 9.09091 | 0.05324 | 0.00056 |
| 0.00032 | 8.65950 | 9.09091 | 0.03065 | 0.00032 |
| 0.00018 | 8.85052 | 9.09091 | 0.01747 | 0.00018 |
| 0.00010 | 8.96109 | 9.09091 | 0.00990 | 0.00010 |
| 0.00006 | 9.02430 | 9.09091 | 0.00559 | 0.00006 |
| 0.00003 | 9.06018 | 9.09091 | 0.00315 | 0.00003 |
| 0.00002 | 9.08046 | 9.09091 | 0.00178 | 0.00002 |
| 0.00001 | 9.09190 | 9.09091 | 0.00100 | 0.00001 |
| LAMBDA1/LAMBDA2= | 1000.0 P= | 0.0010 μ.= | 1.0000 | |
| 0.10000 | 1.09583 | 250.25000 | 0.99010 | 0.09091 |
| 0.05623 | 1.29401 | 250.25000 | 0.98253 | 0.05324 |
| 0.03162 | 1.88197 | 250.25000 | 0.96935 | 0.03065 |
| 0.01778 | 3.54780 | 250.25000 | 0.94676 | 0.01747 |
| 0.01000 | 7.92479 | 250.25000 | 0.90909 | 0.00990 |
| 0.00562 | 18.15977 | 250.25000 | 0.84902 | 0.00559 |
| 0.00316 | 38.42674 | 250.25000 | 0.75975 | 0.00315 |
| 0.00178 | 70.87764 | 250.25000 | 0.64006 | 0.00178 |
| 0.00100 | 111.85199 | 250.25000 | 0.50000 | 0.00100 |
| 0.00056 | 152.97129 | 250.25000 | 0.35994 | 0.00056 |
| 0.00032 | 186.99831 | 250.25000 | 0.24025 | 0.00032 |
| 0.00018 | 211.40121 | 250.25000 | 0.15098 | 0.00018 |
| 0.00010 | 227.29323 | 250.25000 | 0.09091 | 0.00010 |
| 0.00006 | 237.02361 | 250.25000 | 0.05324 | 0.00006 |
| 0.00003 | 242.78979 | 250.25000 | 0.03065 | 0.00003 |
| 0.00002 | 246.11969 | 250.25000 | 0.01747 | 0.00002 |
| 0.00001 | 248.02254 | 250.25000 | 0.00990 | 0.00001 |

Example 3 A system consisting of two components, operating redundantly in parallel. The components are selected together from one of two batches, one with a hazard rate $\lambda_1$, the other with a hazard rate $\lambda_2$. The probability of selection from the first group is p. The system is activated intermittently, with a constant probability intensity $\alpha$. On failure on demand, the system is repaired, with a mean repair time $1/\mu$. This corresponds to some failures of type III.

First solving the problem for a single component model for failure can be established as follows




$$\dot{P}_0(t) = -\lambda P_0(t)$$
$$\dot{P}_1(t) = -\alpha P_1(t) + \lambda P_0(t)$$
$$\dot{P}_2(t) = \alpha P_1(t)$$
$$P_0(t) + P_1(t) + P_2(t) = 1$$

Taking Laplace transforms

$$sP_0(s) - 1 = -\lambda P_0(s)$$
$$s P_1(s) = \lambda P_0(s) - \alpha P_1(s)$$
$$s P_2(s) = \alpha P_1(s)$$

$$P_0(s) = 1/(s+\lambda)$$
$$s P_1(s) = \lambda/s+\lambda - \alpha P_1(s)$$
$$\frac{s^2 P_2(s)}{\alpha} = \frac{\lambda}{s+\lambda} - S P_2(s)$$
$$P_2(s) = \frac{\lambda\alpha}{s(s+\lambda)(s+\alpha)}$$
$$P_2(t) = 1 + \frac{\alpha}{\lambda-\alpha} e^{-\lambda t} - \frac{\lambda}{\lambda-\alpha} e^{-\alpha t}$$

density function

$$p_2(t) = \frac{\lambda\alpha}{\lambda-\alpha} e^{-\alpha t} - \frac{\lambda\alpha}{\lambda-\alpha} e^{-\lambda t}$$

$$MTTF = \int_0^\infty t\, p(t)\, dt$$

$$= \frac{\lambda\alpha}{\lambda-\alpha}\left(\frac{1}{\alpha^2} - \frac{1}{\lambda^2}\right)$$

$$= \frac{1}{\alpha} + \frac{1}{\lambda}$$

$$\lim_{t\to\infty} \text{Unavailability } (t) = \frac{MTTR}{MTTF + MTTR}$$

(Gnedenko et al. 1969)

$$\text{then } U = \frac{1/\mu}{1/\mu+1/\alpha+1/\lambda}$$

For two components, we have $U_1$ is unavailability for components from batch 1, $U_2$ for batch 2.

$$C_{UA,2} = \frac{p\, U_1^2 + (1-p)\, U_2^2}{(p\, U_1 + (1-p)\, U_2)^2}$$

$$C_{UA,2} = \frac{p\,\left(\frac{U_1}{U_2}\right)^2 + 1-p}{\left(p\left(\frac{U_1}{U_2}\right) + 1-p\right)^2}$$

This gives results very similar to those for example 2.

## 6. SIMILAR COMPONENT COUPLED FAILURES - DATA

The data presented here are drawn from two other studies, of design errors and multiple failure incidents. In Risø-M-1742, first some design error failures were classified, then data from abnormal occurrences in boiling water reactors during one year, and data from Reactor Operating Experiences during one year were classified. All of these studies yielded information on the ratio of similar component coupled failures to single component failures. However, since the different failures were not classified by component type, the data serves only to indicate the degree to which coupled failure might be important. Some of the results are repeated here in table 1.

In Risø-M-1837, results of a study of all available abnormal occurrence reports from five reactors were presented, showing an analysis of causes of failures, and recording the number of multiple failure incidents. In parallel with the results presented there, a study of similar component coupled failures was performed. The results from that study are presented here. In all, a total of 340 abnormal occurrences were studied here. The number of failures was higher, because some of the abnormal occurrences involved several failures.

The results of the study are presented in table 2. Some attempt has been made to record the number of components at risk, where such information was available. Multiple similar component failures are marked as N/M, N expressing the number of components failing, M the number at risk. So $3 \times \frac{2}{3}$ means there were three cases in which two components failed when three were at risk.

The similar component coupled failures are classified as types I, II and III. There was only one case in which a type IV failure occurred.

Of the 422 independent failures recorded (failures of several components of the same type due to the same cause are not independent), 121 involved actual coupled failures. 24 involved situations where only one of a group of components failed to function, but where several components of the same type were affected by the same mechanisms. This means that 29% of all independent failures were coupled failures involving two or more components. 34% of all failures involved coupled failure effects. (Table 2).

A good many of the coupled failures occurred in components with a long history of high failure rates. It could be argued that once such problem components are identified, reliance on them ceases, until identification of the cause of the problem is made, and the failure mechanism removed. If data for these types of components are removed from the data, the number of coupled failures is reduced, to 78 or 18.5%.

It should be noted that in many instances of single failures, it was not possible to determine the number of components at risk. In some few cases, only one component of a particular type was at risk. In such cases, simular component coupled failures are impossible. If one regards the proportion of coupled failures as a property of the particular component type, then the "natural" proportion of coupled failures will tend to be underestimated, from the data given here. This fact will be important if one tries to transfer the use of this data to power plants in which redundancy practice is different from the plants studied here.

| Failure cause | No common mode effect | Common mode effect. No common mode consequence | common mode consequence |
|---|---|---|---|
| Design | 5 | 7 | 14 |
| 26 | 19% | 27% | 54% |
| Operation | 3 | 0 | 0 |
| Component* | | | |
| Procedure | 4 | | 2 |
| Installation/ maintenance | 9 | | 2 |
| Total | 35 | 8 | 22 |
| 65 | 54% | 12% | 34% |

* Incidents were classified as component failures if no design modifications were made. Common mode failures would result in immediate modification, if the failures in themselves threatened safety and would hence be defined as design errors.

Table 1. Common mode effects for two reactors during one year. (Risø-M-1742, 1974, P 62)

For this table, all available abnormal occurrence reports for two reactors during one year were studied, and individual failures were classified according to their cause and degree of coupling involved. Note that some systems were not redundant, and that similar component common mode failures alone were considered.

| Component Type | Failure mechanism type * | | | Number of coupled failures | Number of single failures |
|---|---|---|---|---|---|
| | Type I | Type II | Type III | | |
| Manual control or shut off valve | | 3×1<br>1×2/2 | 3×1<br>1×3/3 | 2 | 6 |
| Current trip relay | | 1×3/3 | | 1 | |
| Flow switch | 1×2/2 | 2×1<br>3×2/2<br>1×4/4 | | 5 | 2 |
| Control rod | 1×26/26<br>1×3/Many | 6×1/Many<br>2×2/Many<br>4×3/Many<br>1×6/Many | | 9 | 6 |
| Neutron Monitor | | 2×1 | 2×1<br>1×2/2<br>1×Many/Many | 2 | 4 |
| Motor driven fan | | 1×2/2<br>1×1 | | 1 | 1 |

Table 2. Failures from Abnormal occurrence reports for five reactors (see Risø-M-1742) classified according to component and coupled failure type.

L x M/N means L cases in which M components failed out of a total of N.

* See page 8 and figure 11 for definitions.

| Component Type | Failure mechanism type | | | Number of coupled failures | Number of single failures |
|---|---|---|---|---|---|
| | Type I | Type II | Type III | | |
| Storage battery | | 1×2/2 | | 1 | |
| Draft control damper | | 1×4/4 | | 1 | |
| Torque switch | | 2×1 | | | 2 |
| Temperature switch | | 2×1 | | | 2 |
| Motorised valve | 1×2/2 | 21×1 (The only non coupled i.e. random double failure recorded was in this group) | | | |
| | | 1×2/2<br>1×4/4 | | 3 | 21 |
| Pump control | 1×2/2 | | | 1 | |
| Check valve | | 1×1 | | | 1 |
| Timerrelay | | 2×1<br>1×2/2<br>1×3/3 | | 2 | 2 |
| Containment control complex | 1×2/2 | | | 1 | |

L x M/N means L cases in which M components failed out of a total of N.

| Component Type | Failure mechanism type | | | Number of coupled failures | Number of single failures |
|---|---|---|---|---|---|
| | Type I | Type II | Type III | | |
| MSIV (Main steam isolation valve) | | 15×1<br>1×2/4<br>1×1/3<br>1×3/4<br>1×4/4 | | 4 | 15 |
| Pressure switch | | 17×1/4<br>5×2/3<br>1×3/3<br>5×2/4 | | 11 | 17 |
| Solenoid valve | | 7×1<br>1×2/2<br>1×2/Many<br>1×3/3<br>1×3/Many | | 4 | 7 |
| Relief & Safety valves | | 3×1<br>2×4/16<br>1×2/M | | 3 | 3 |
| Vacuum Breaker valve | | 2×1/Many<br>1×2/2<br>1×2/4<br>3×4/4 | | 5 | 2 |

L x M/N means L cases in which M components failed out of a total of N.

| Component Type | Failure mechanism type | | | Number of coupled failures | Number of single failures |
|---|---|---|---|---|---|
| | Type I | Type II | Type III | | |
| Measuring relay | | 15×1<br>3×2/2 | | 3 | 15 |
| Core spray system (water hammer) | 2/2 | | | 1 | |
| Switch | | 3×1<br>1×2/4 | | 1 | 3 |
| Steam generator | | 1×2/4, 1×3/4<br>3×1 | | 2 | 3 |
| Circuit breaker | | 3×2/4, 1×2/2<br>1×3/4, 1×1/4 | | 5 | 1 |
| Boric acid pump | | 5×1/2 | A remarkable sequence in which alternate pumps failed in every other test 5 | | |
| Diesel generator | | 17×1<br>4×2/2 | | 4 | 17 |

L x M/N means L cases in which M components failed out of a total of N.

## 7. CONCLUSION

One conclusion from this study is that there is a sufficient number of coupled failures to make collection of statistical data worthwhile. The actual data collected served to indicate the kind of components for which data collection would be worthwhile, rather than as a basis for statistical estimates. The data are too sparse to provide other than order of magnitude estimates of reliability.

The other conclusion must be that classification of coupled failures is difficult. For this reason, it is recommended that data should be recorded whenever several components of the same type fail to function, without distinguishing whether a common mode effect is involved, or whether the failures were independent. Further classification is then desirable as far as is possible since the different types have very different characteristics, for example with respect to the effect of increasing the frequency of testing.

From looking at the ratios of coupled failures to single failures found in practice, it can be seen that in by far the majority of cases the values lie in the range 1/2 to 1/20. It should be remembered that the samples given are often very small, and that data have been collected only for components which are highly susceptible to coupled failure. For example, there are very few electronic components represented in the data collection.

From the calculations, it can be seen that for twofold redundant systems, the biggest discrepancy between reliability values, calculated with and without taking account of coupled failure, is found for those components which individually have very high reliabilities, and for which coupled failures are rare.

The worst discrepancies between calculations with and without coupled failure would arise with component with very low unavailabilities - electronic circuits for example. If into this situation a small "bad batch" is introduced, the discrepancy between calculations can be large. The "bad batch" should be small, so that the excess failures it causes do not make a significant change in the overall failure rate data for single

components. And the failure rates in the "bad batch" should not be so high, that the poor components are detected during early testing. Then, to use such components in twofold or threefold redundancy can produce large failure rate prediction discrepancies.

This kind of reasoning, though derived from just simple cases of coupled failure, focusses attention on failure rate distributions. One method of calculating common mode failure probability (WASH1400, Appendix IV) is to fit a distribution to failure rate estimates derived from several different sources, and to sample this distribution repeatedly to provide data for monte carlo simulations of plant reliability. Some of the examples show how critical the step of deriving a failure rate distribution.

## 8. REFERENCES

Epler, E.P., 1969: Common mode failure considerations in the design of systems for protection and control. Nuclear Safety, Vol. 10 No. 1.

Rasmussen, N. el al.: An assessment of accident risks in U.S. Commercial nuclear power plants. Appendix IV Common mode failure WASH 1400 Draft 1974.

Gangloff, W.C.: Common mode failure analysis IEEE Trans. on power apparatus and systems, Vol. PAS-94 No. 1 p 27-30, Jan/Feb 1975

Taylor, J.R.: Design errors in nuclear power plant, Report Risø-M-1742, 1974.

Taylor, J.R.: A study of abnormal occurrences in nuclear power plant, Report Risø-M-1837, 1975.